

Fig. 1

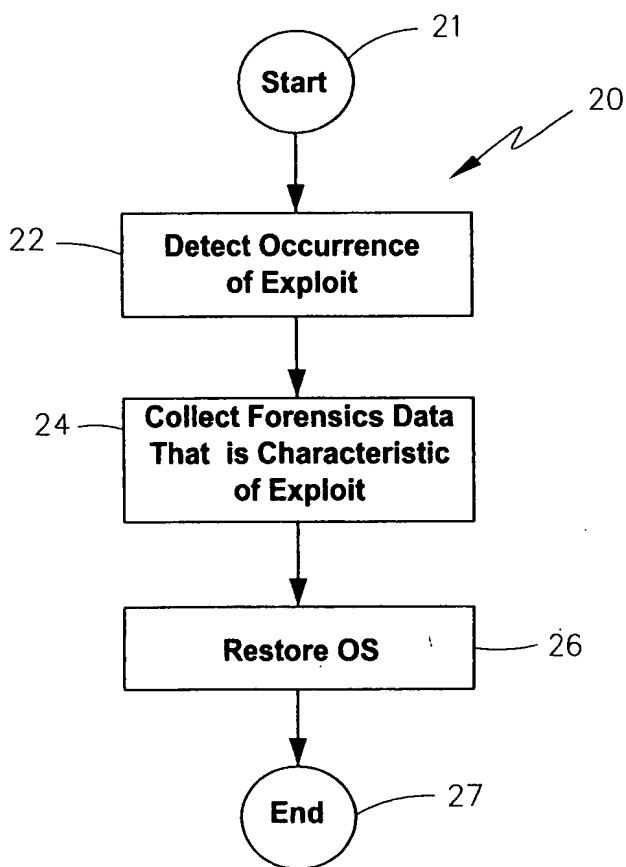


Fig. 2

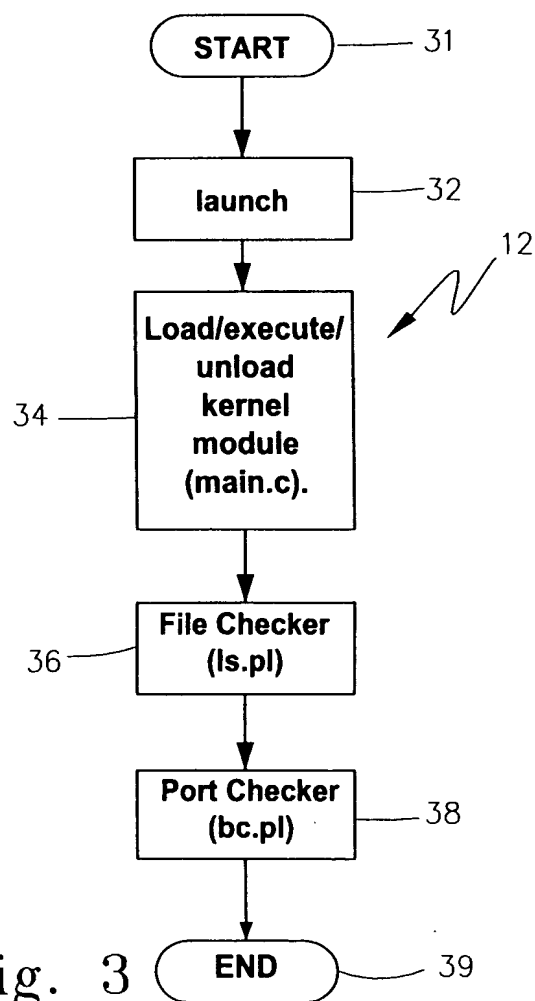


Fig. 3

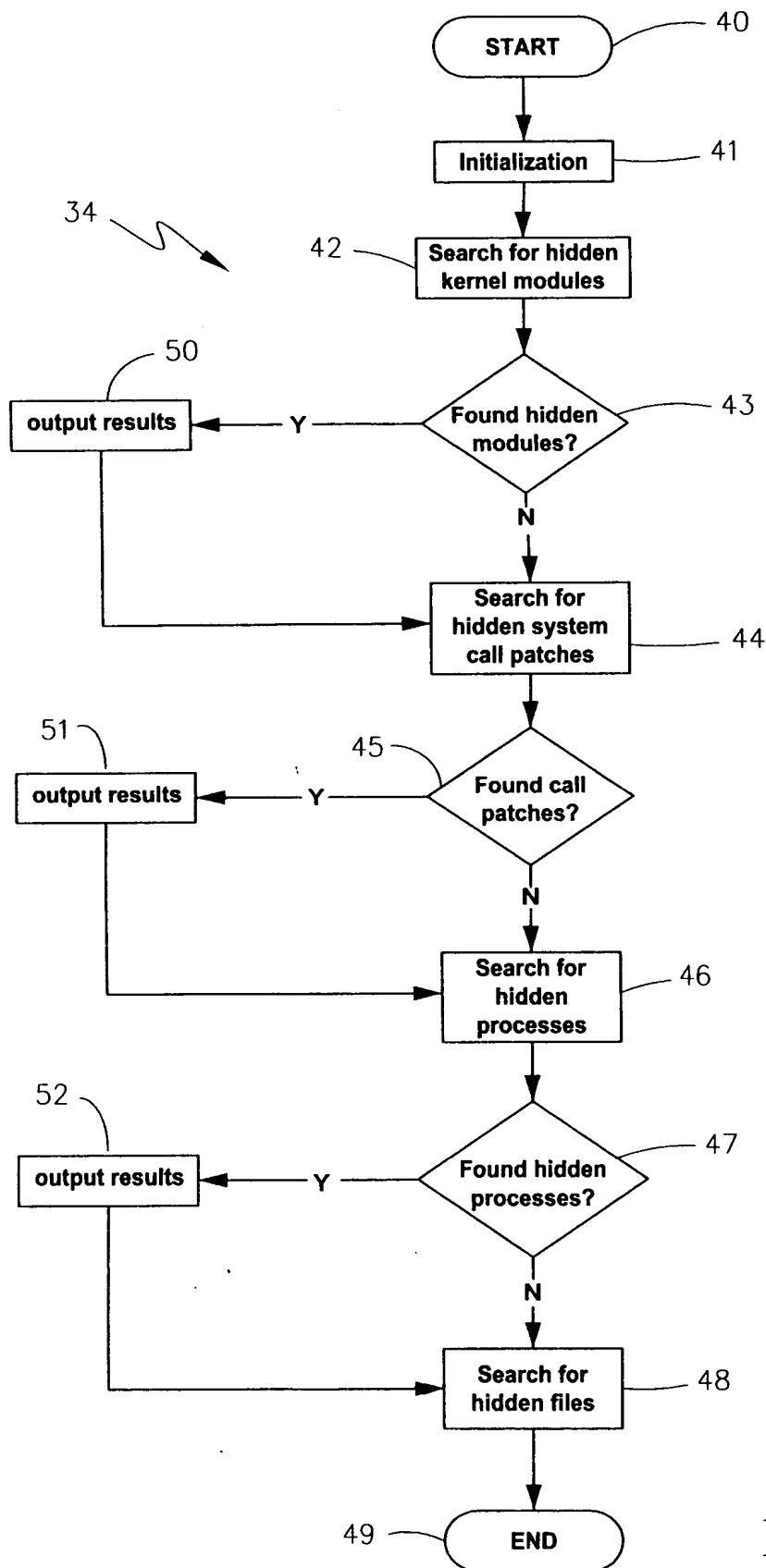


Fig.4

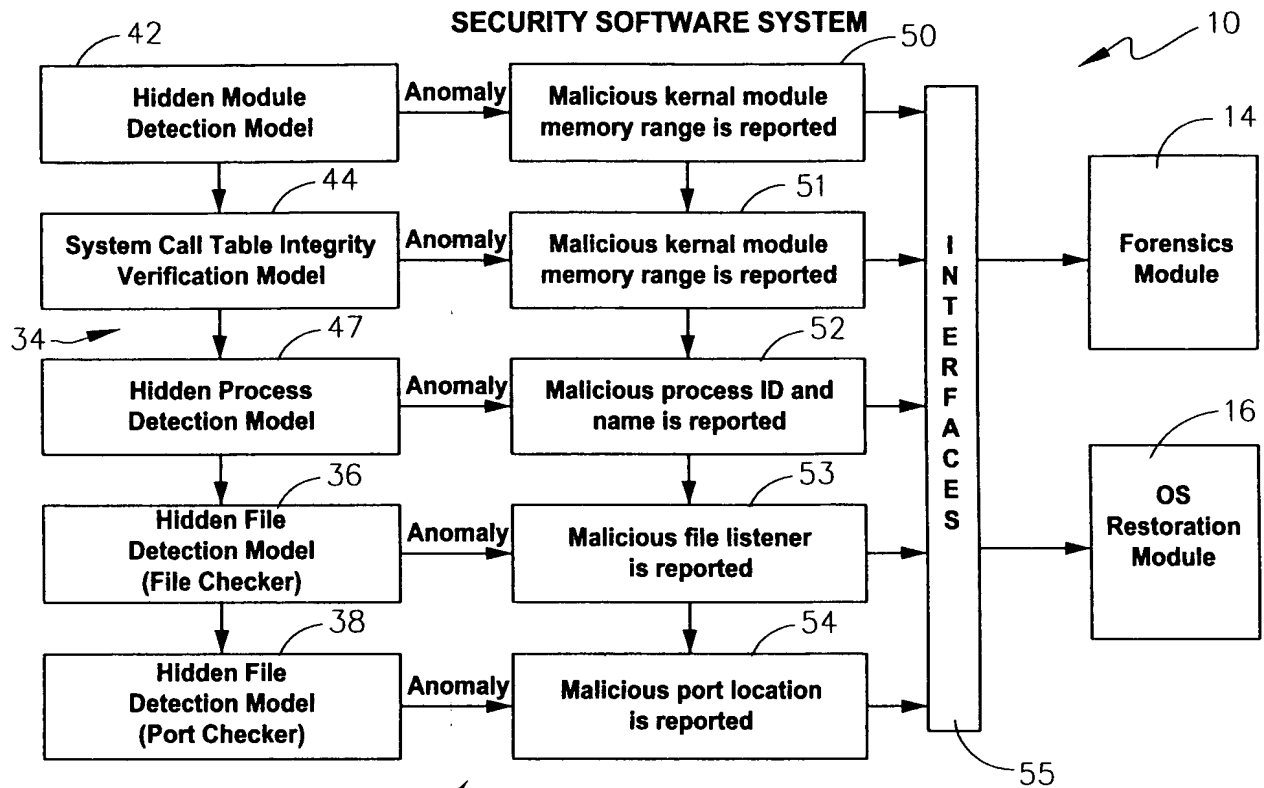


Fig.5

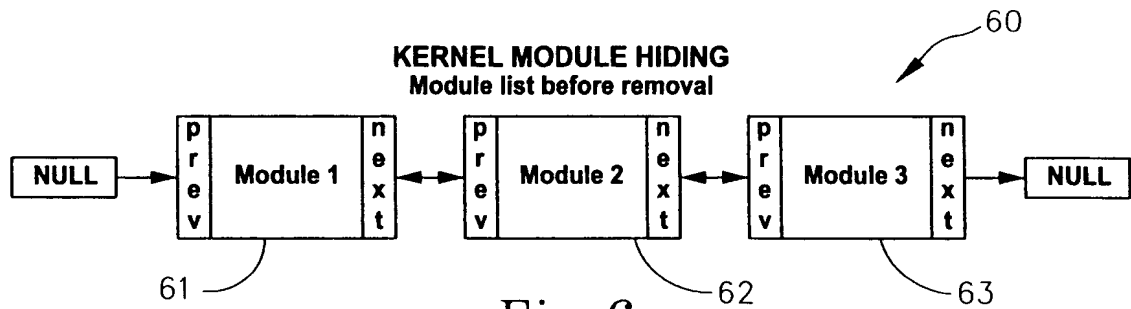


Fig.6a

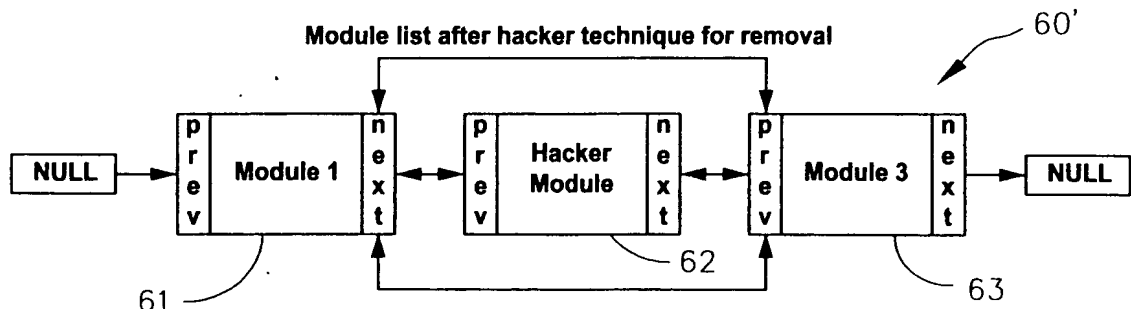


Fig.6b

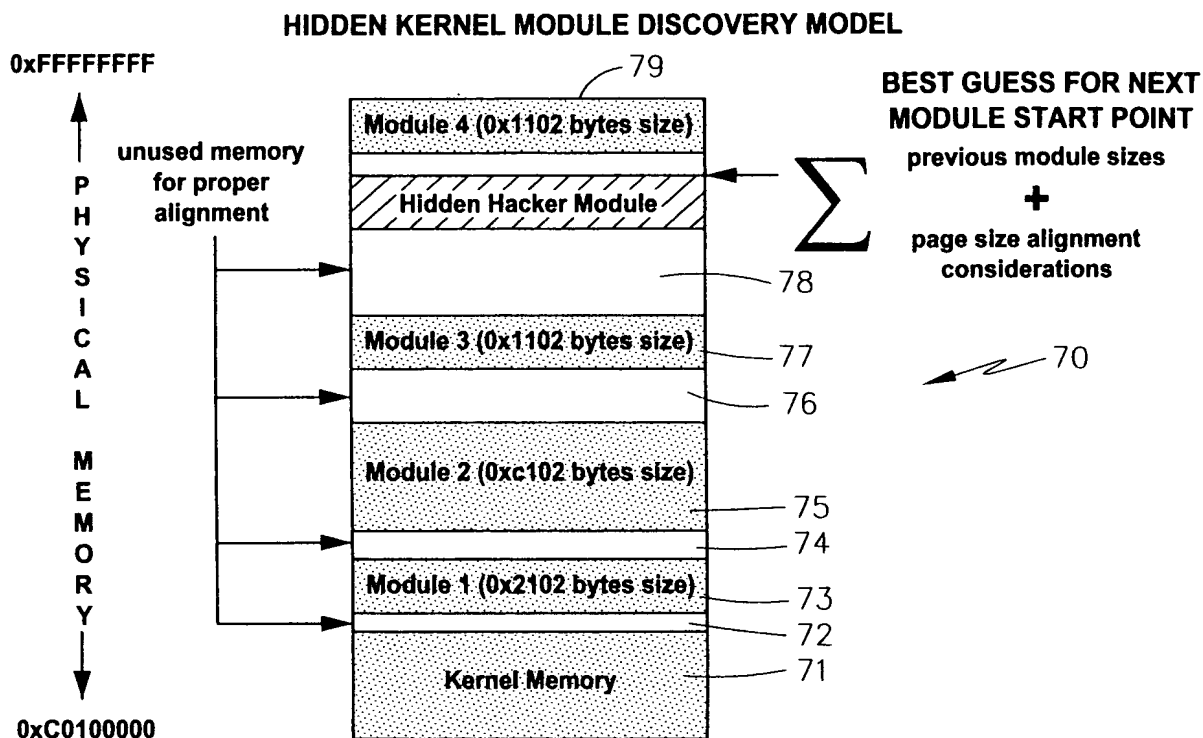


Fig.7

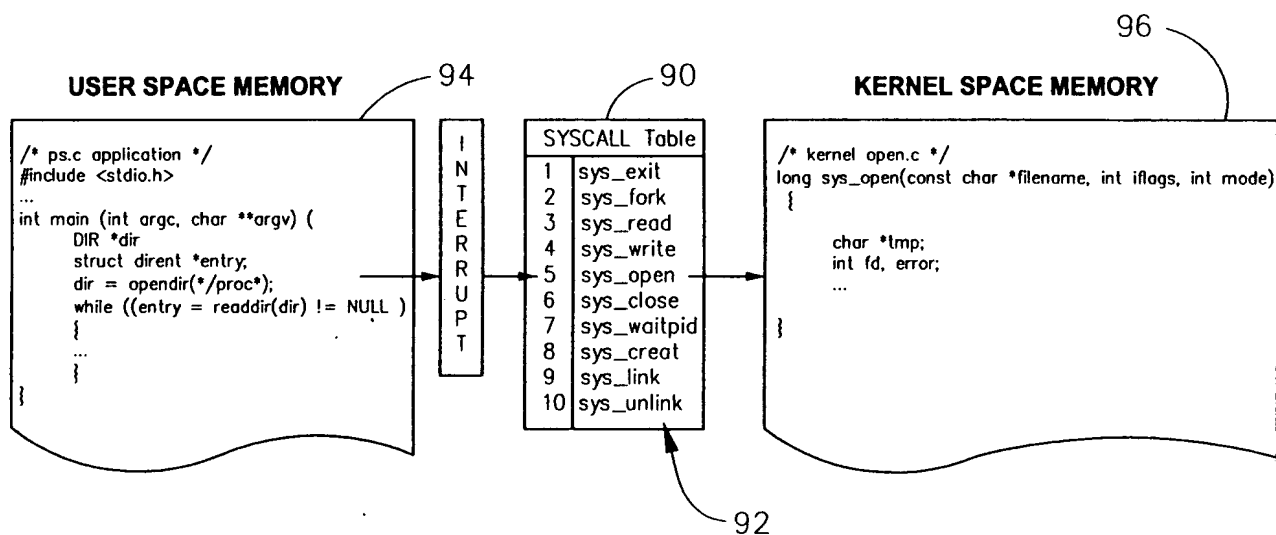


Fig.9

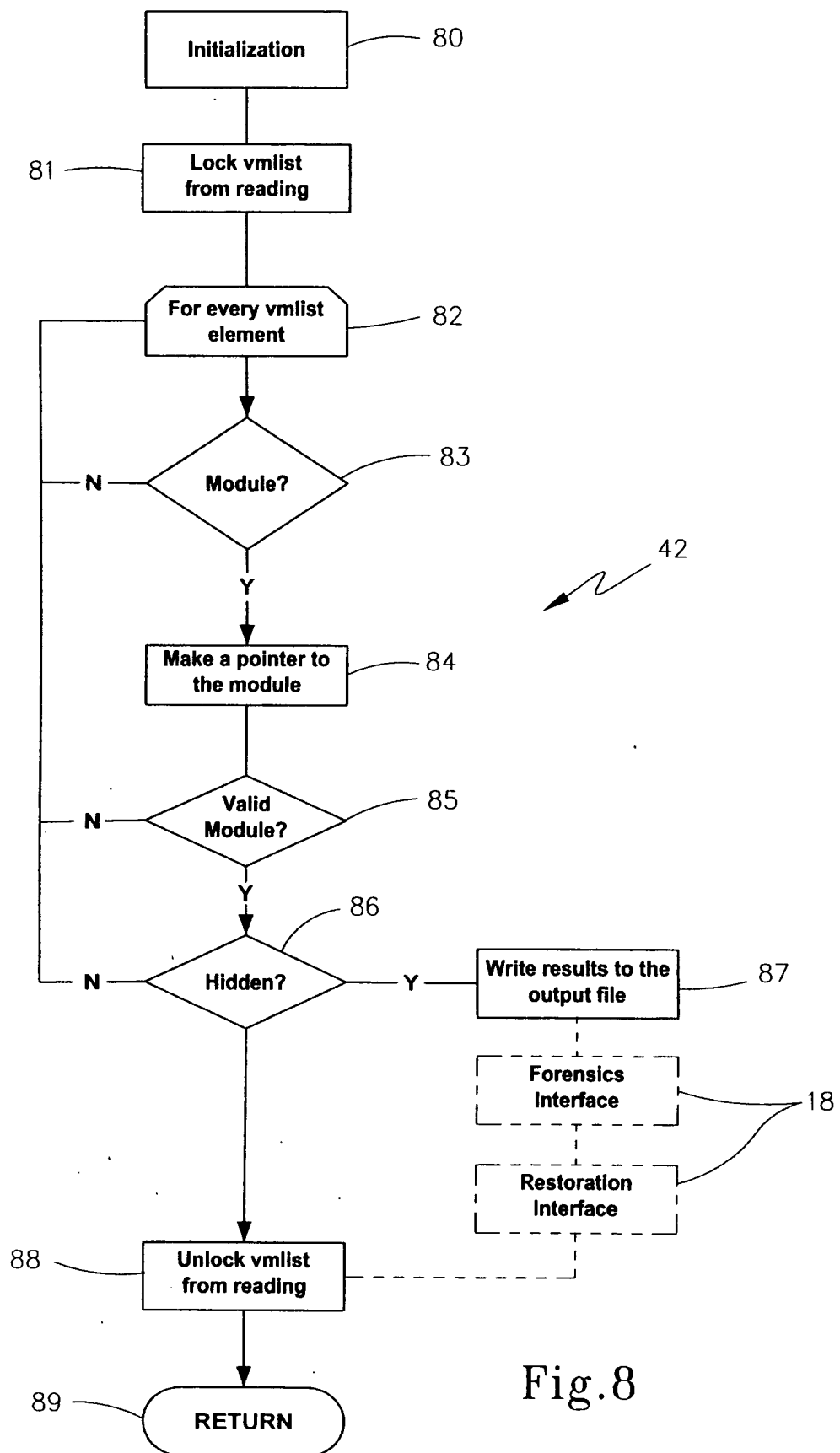


Fig.8

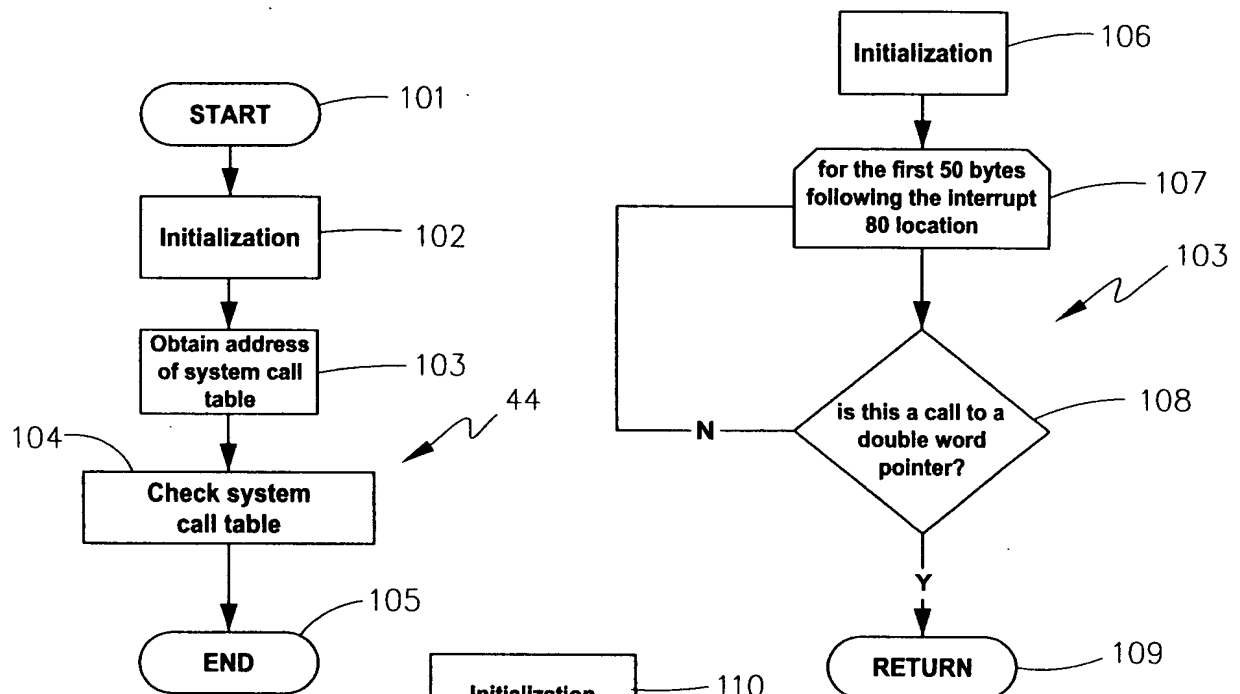


Fig. 10a

Fig. 10b

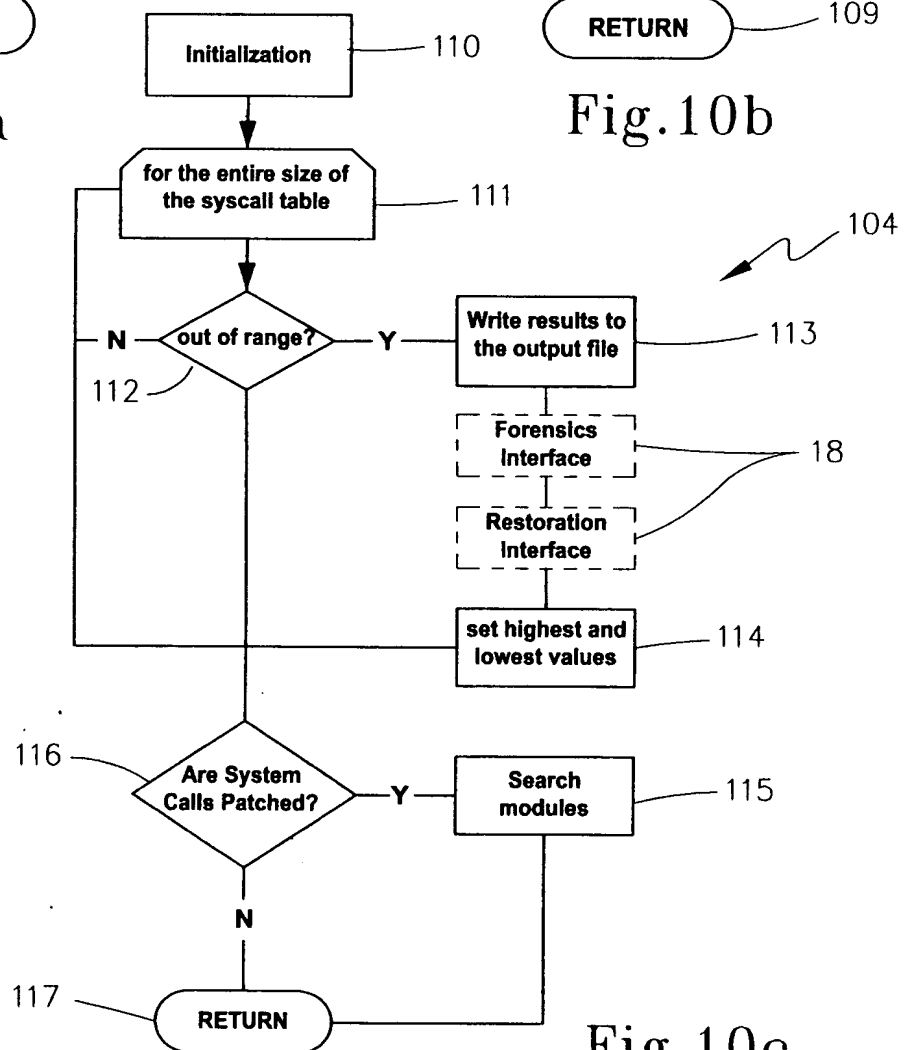


Fig. 10c

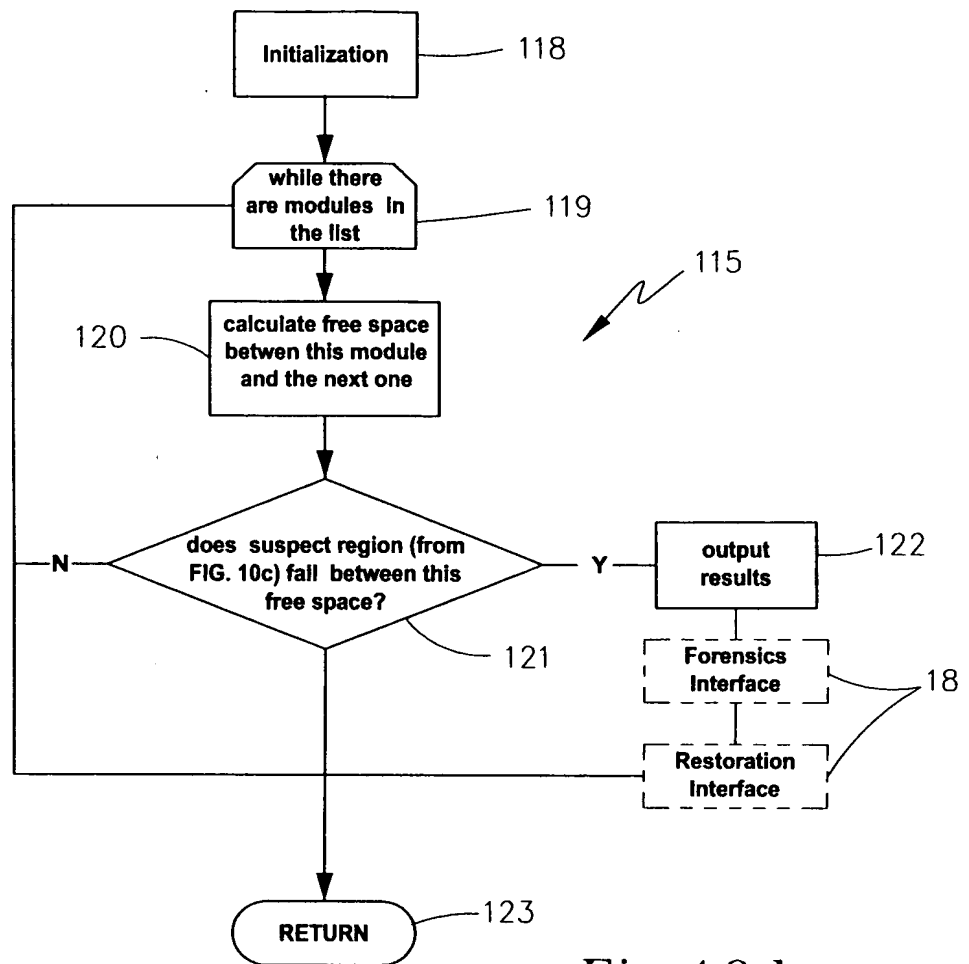
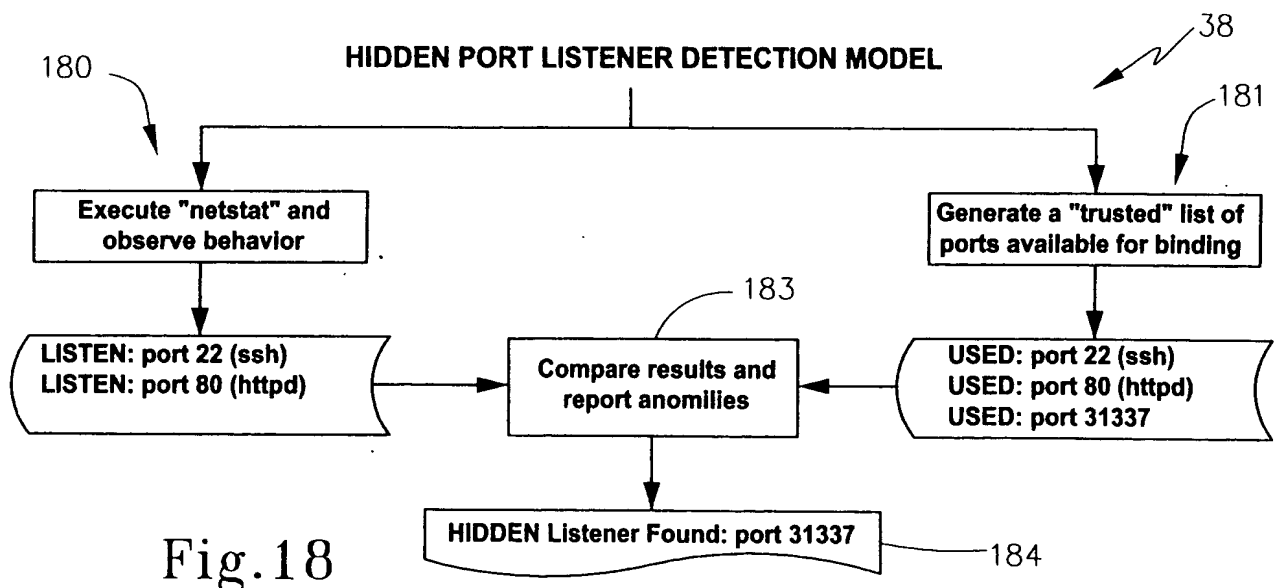
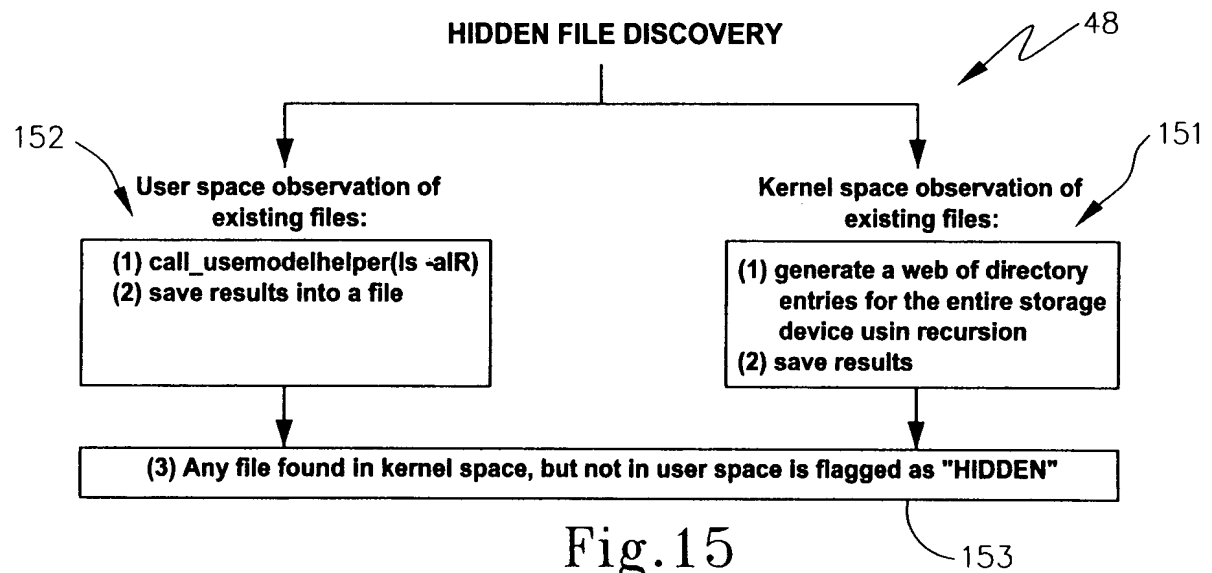
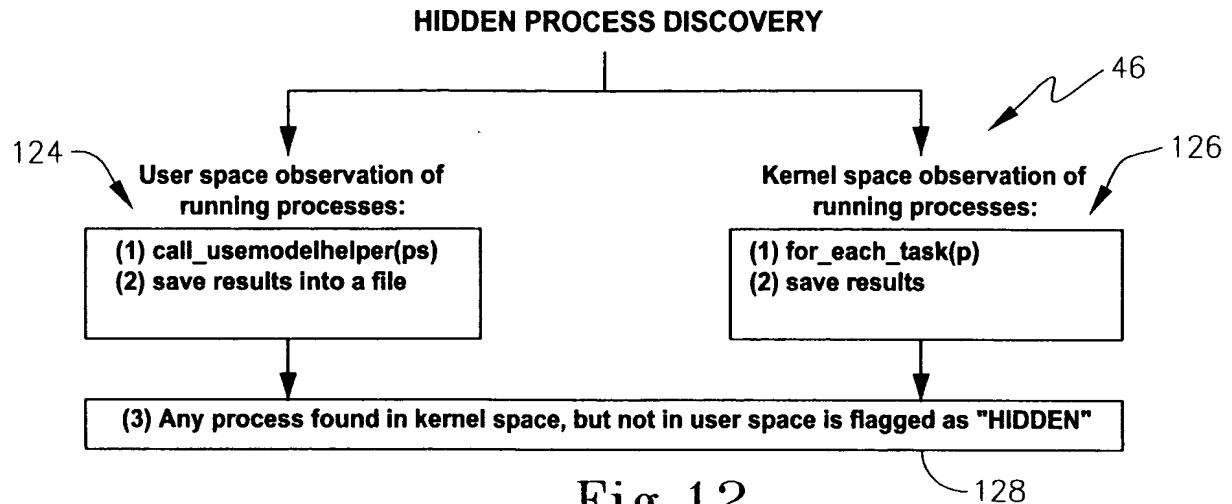


Fig.10d

IDENTIFIED SYSCALL ANOMALIES CAUSE BY ADORE v0.42

| | | | | | |
|---------------|------------|--------|------------|---------|---|
| syscall [2] | fork | FAILED | 0xf8aca650 | Highest | <div>analyze_memory (highest, lowest) { if the range falls between two valid kernel modules then flag the entire memory range in between the two as a malicious kernel module. }</div> |
| syscall [4] | write | FAILED | 0xf8aca7e8 | | |
| syscall [5] | open | FAILED | 0xf8acb184 | | |
| syscall [6] | close | FAILED | 0xf8aca898 | | |
| syscall [18] | oldstat | FAILED | 0xf8acabe4 | | |
| syscall [37] | kill | FAILED | 0xf8aca710 | | |
| syscall [39] | mkdir | FAILED | 0xf8aca9a0 | | |
| syscall [84] | oldlstat | FAILED | 0xf8acacd0 | | |
| syscall [106] | stat | FAILED | 0xf8acadb0 | | |
| syscall [107] | lstat | FAILED | 0xf8acae94 | | |
| syscall [120] | clone | FAILED | 0xf8aca6b0 | | |
| syscall [141] | getdents | FAILED | 0xf8aca368 | Lowest | |
| syscall [195] | stat64 | FAILED | 0xf8acaf80 | | |
| syscall [196] | lstat64 | FAILED | 0xf8acb080 | | |
| syscall [220] | getdents64 | FAILED | 0xf8aca4dc | | |

Fig.11



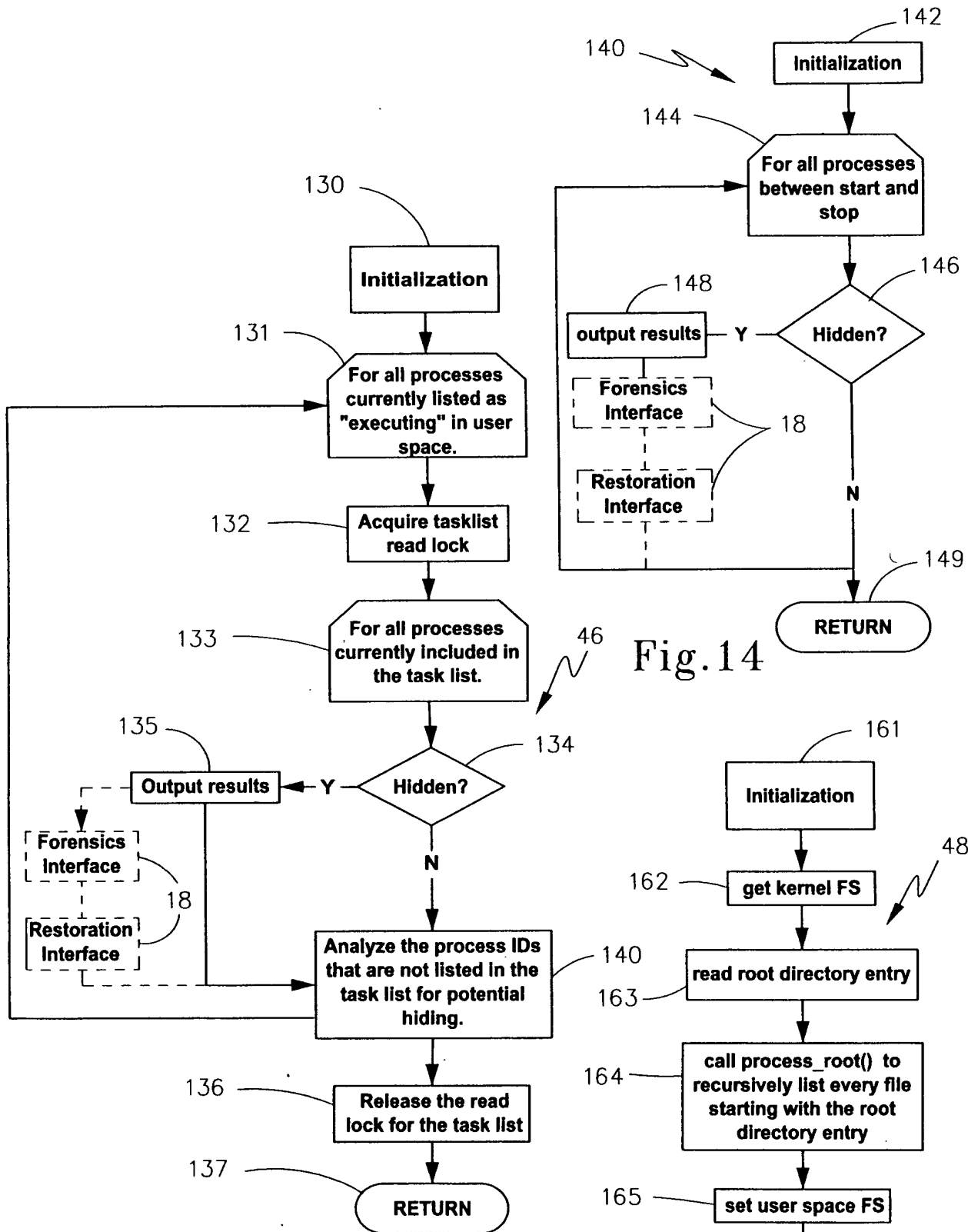


Fig.13

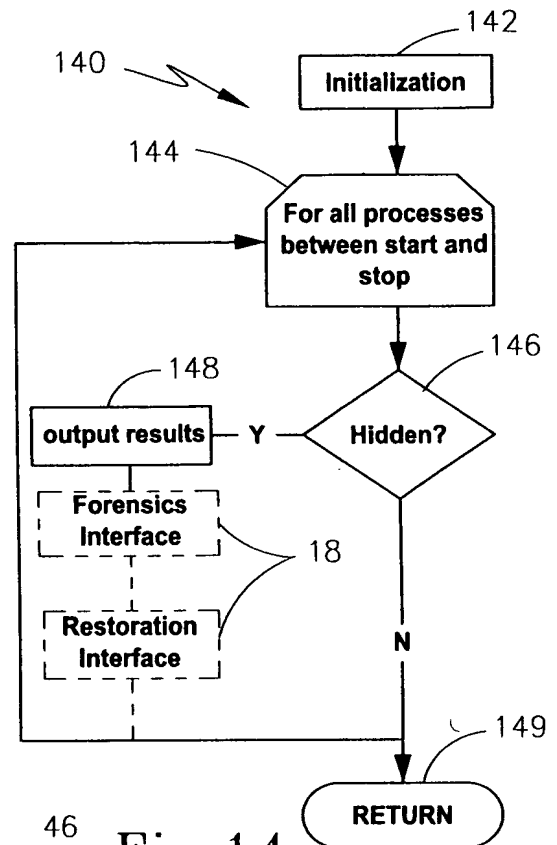


Fig.14

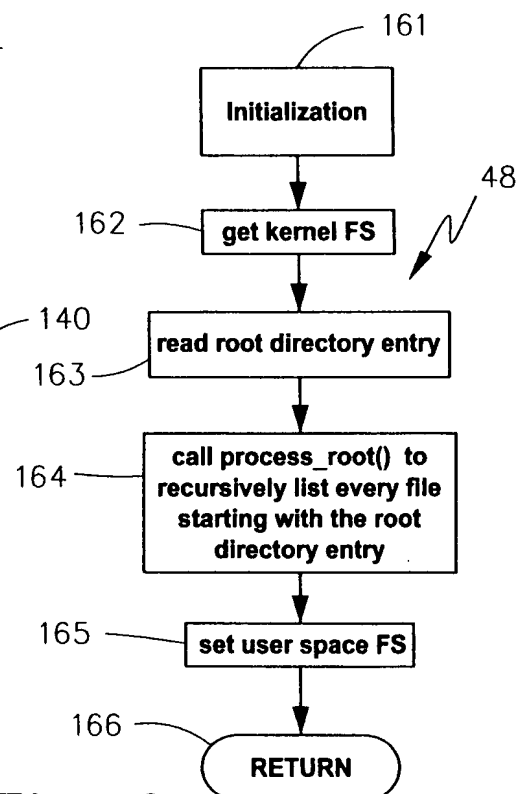


Fig.16

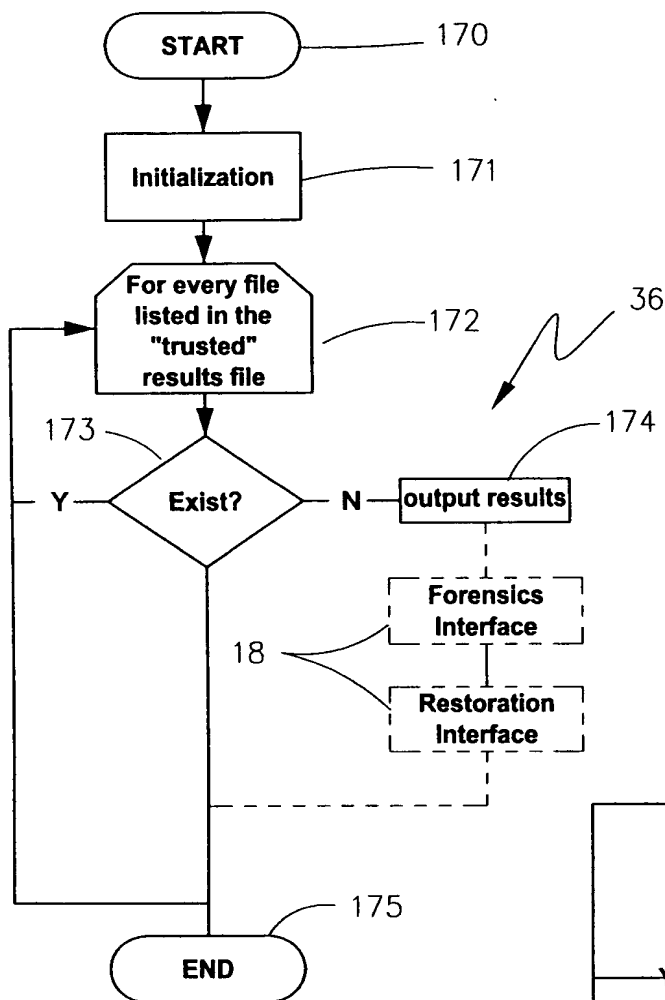


Fig. 17

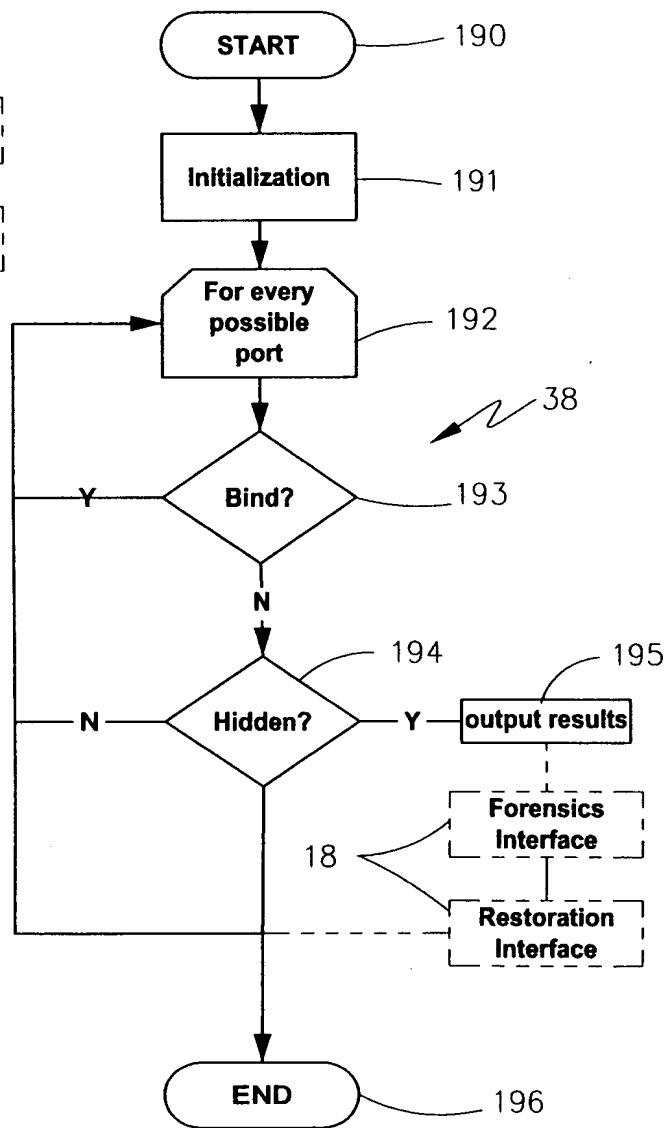


FIG. 19

```
Script started on Sat Aug 9 15:42:00 2003
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator- this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]
```

```
-----[ SUMMARY ]-----
NO hidden modules were found.
NO system call table modifications were found.
NO hidden processes were found.
WARNING: File size is 60133 (should be 58885): /var/log/sa/sa09
WARNING: File size is 1010871 (should be 1010003) : /var/log/cron
WARNING: File size is 597700 (should be 597264): /var/log/maillog
NO hidden files were found.
NO hidden TCP port listeners were found.
[root@localhost interrogator]# exit
Script done on Sat Aug 9 16:01:52 2003
```

Fig.20a

```
(root@localhost interrogator) # ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator- this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]
```

```
-----[ SUMMARY ]-----
NO hidden modules were found.
NO system call table modifications were found

WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/de.rojansans/tb
FOUND 1 Hidden process listing

HIDDEN file found: /tmp/hideme
WARNING: File size is 62629 (should be 61381): /var/log/sa/sa09
WARNING: File size is 1013693 (should be 1012816): /var/log/cron
WARNING: File size is 599450 (should be 599012): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```

Fig.20b

```
(root@localhost interrogator)# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-----[ SUMMARY ]-----
WARNING suspect module found: f8a0f000 8000 bytes (adore)
Image stored at /tmp/interrogator/adore.o
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]      FAILED  0xf8a0f650      fork
syscall[41]     FAILED  0xf8a0f7e8      write
syscall[5]      FAILED  0xf8a0f184      open
syscall[6]      FAILED  0xf8a0f898      close
syscall[18]     FAILED  0xf8a0fbe4      oldstat
syscall[37]     FAILED  0xf8a0f710      kill
syscall[39]     FAILED  0xf8a0f9a0      mkdir
syscall[84]     FAILED  0xf8a0fcd0      oldlstat
syscall[106]    FAILED  0xf8a0fdb0      stat
syscall[107]    FAILED  0xf8a0fe94      lstat
syscall[120]    FAILED  0xf8a0f6b0      clone
syscall[141]    FAILED  0xf8a0f368      getdents
syscall[195]    FAILED  0xf8a0ff80      stat64
syscall[196]    FAILED  0xf8a0f080      lstat64
syscall[220]    FAILED  0xf8a0f4dc      getdents64
Suspect module located (0xf89da6d8 - 0xf8a2000)
FOUND 15 Modified syscall table functions

WARNING: Found process id 836 removed from the task_queue.
Launch Path: /root/code/interrogator/demo/trojans/test
WARNING: process id 13745 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 2 Hidden process listings

HIDDEN File found: /mp/hideme
WARNING: File size is 2336990 (should be 2335392): /var/log/messages

HIDDEN TCP Port Listener found: port 111
HIDDEN TCP Port Listener found: port 139
HIDDEN TCP Port Listener found: port 2222
HIDDEN TCP Port Listener found: port 6000
HIDDEN TCP Port Listener found: port 32768
HIDDEN TCP Port Listener found: port 32769

[root@localhost interrogator]# exit
```


204

Fig.20c

```
[root@localhost interrogator]# ./interrogator
Where would you like the results stored? [/tmp/interrogator/]
Check for hidden processes? [Y]
Check for hidden TCP port listeners? [Y]
Check for system call patching? [Y]
Check for hidden kernel modules? [Y]
Check for hidden files? (may take > 15 minutes) [N] Y
Running the interrogator... this may take a minute
Results are located at /tmp/interrogator/summary
View results now? [Y]

-----[ SUMMARY ]-----
WARNING suspect module found: f8a10000 184700 bytes (homegrown)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[3]      FAILED  0xf8a11494      read
syscall[51]     FAILED  0xf8a11020      open
syscall[11]     FAILED  0xf8a10ebc      execve
syscall[13]     FAILED  0xf8a118a0      time
syscall[78]     FAILED  0xf8a1183c      getlineofday
syscall[141]    FAILED  0xf8a11544      getdents
syscall[220]    FAILED  0xf8a116c0      getdents64

Suspect module located (0xf89db6d8 - 0xf8a3f000)
FOUND 7 Modified syscall table functions

WARNING: process id 1584 hidden or just exited (tb)
Launch Path: /root/code/interrogator/demo/trojans/tb
FOUND 1 Hidden process listing

HIDDEN File found: /tmp/hideme
WARNING: File size is 1021523 (should be 1020648): /var/log/cron
WARNING: File size is 603820 (should be 603384): /var/log/maillog

HIDDEN TCP Port Listener found: port 2222
[root@localhost interrogator]# exit
```


206

Fig.20d

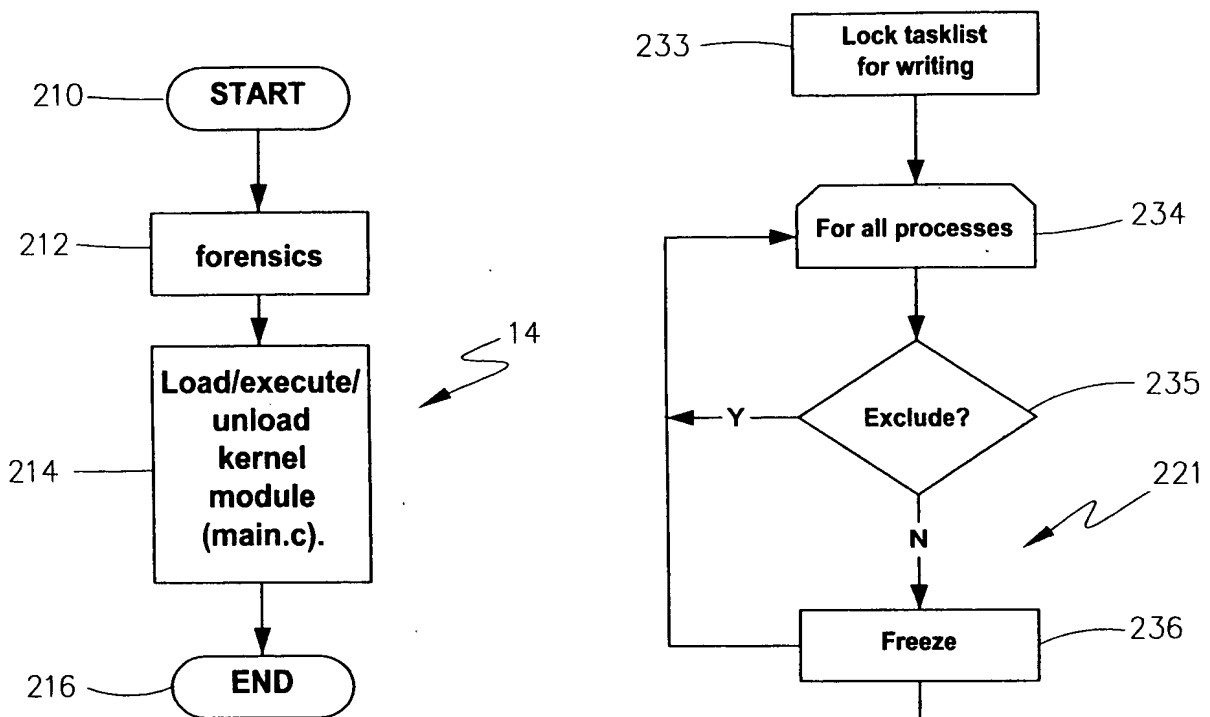


Fig. 21

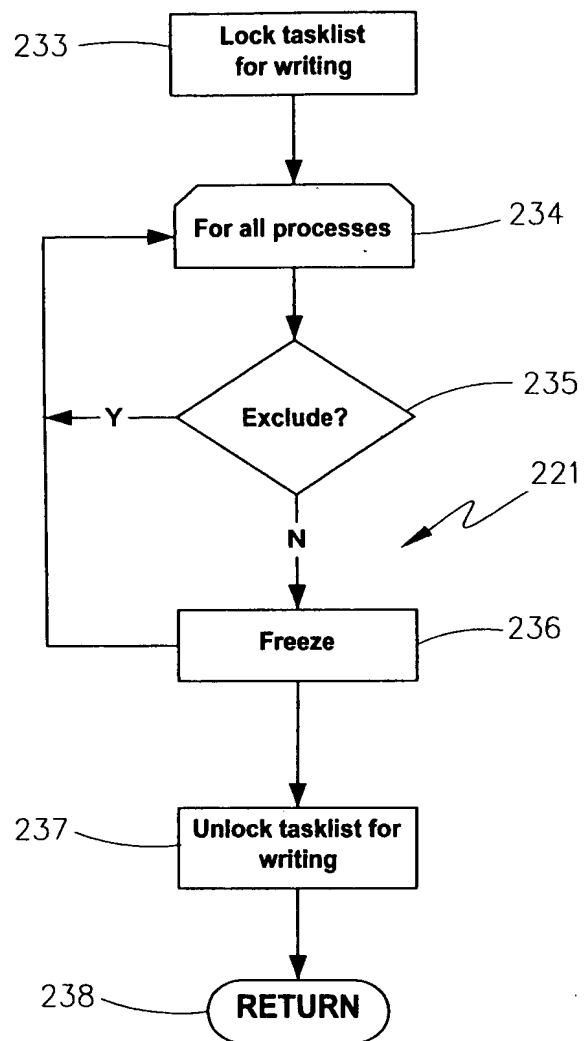


Fig. 23

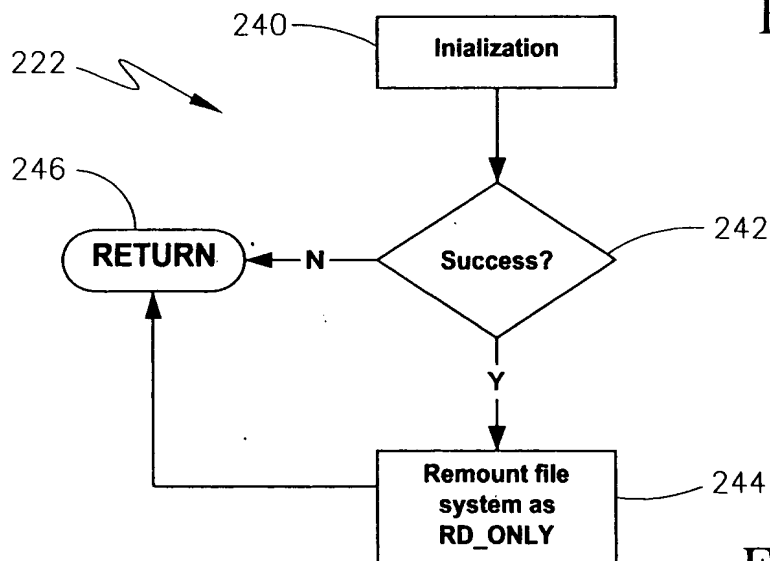


Fig. 24

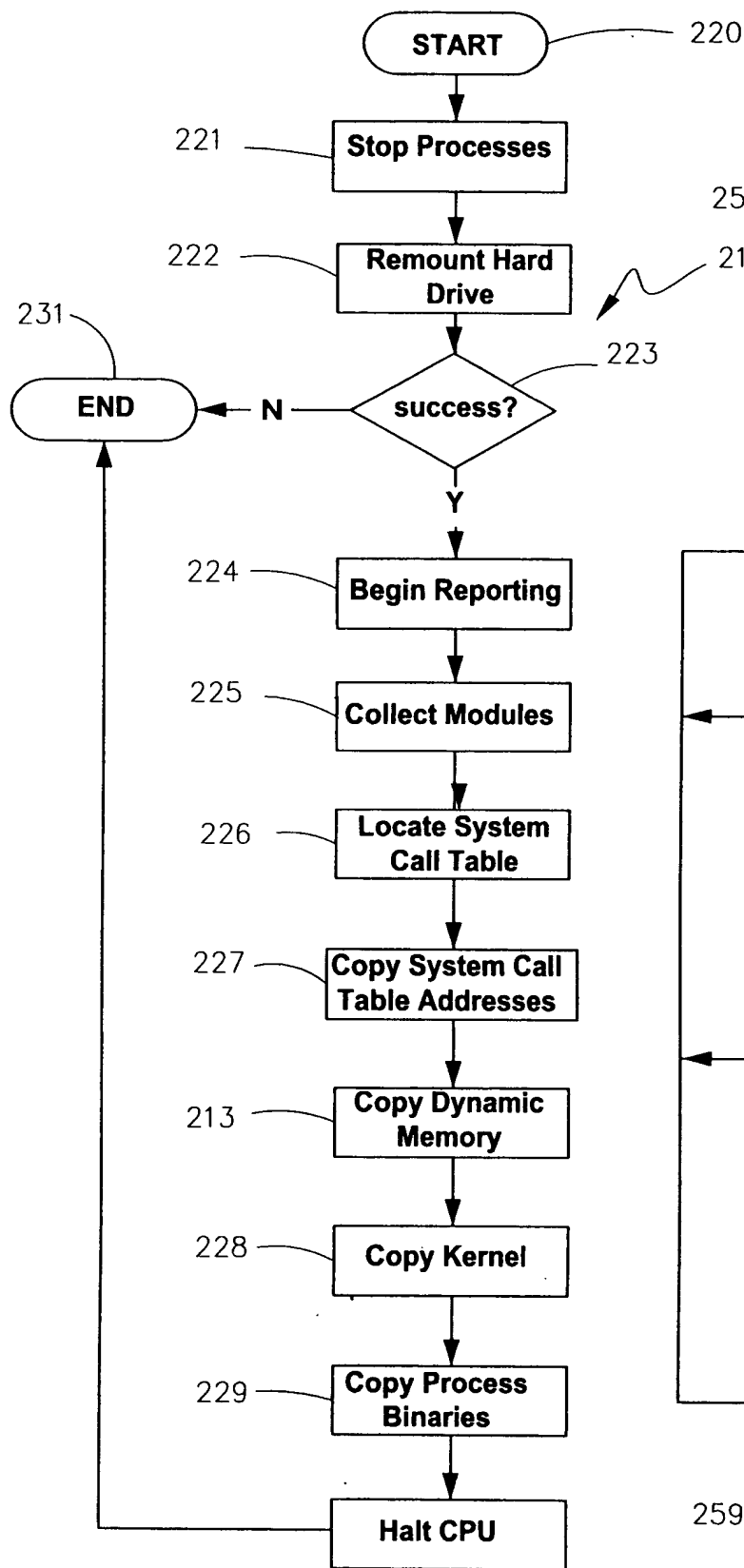


Fig. 22a

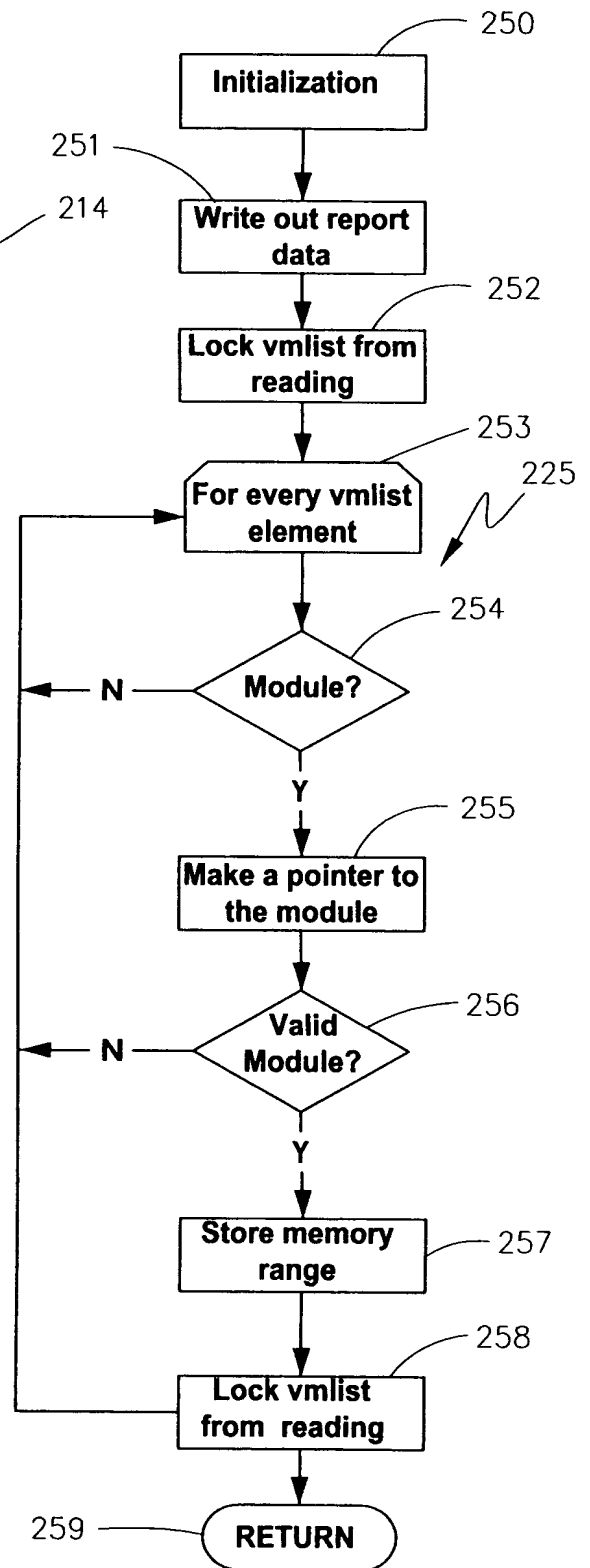


Fig. 25a

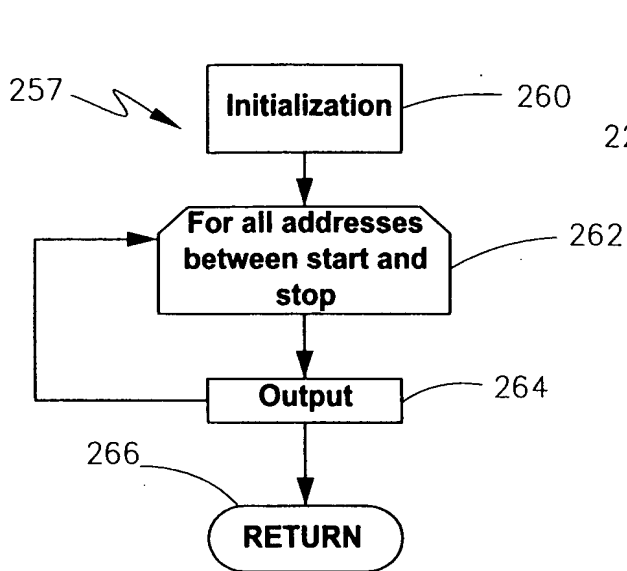


Fig.26

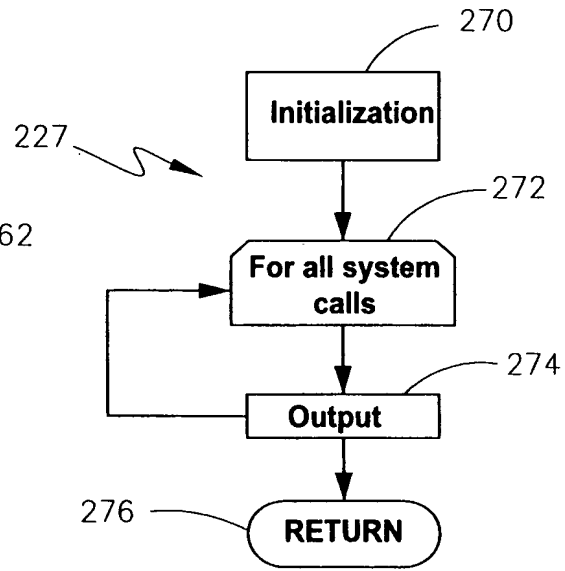


Fig.27a

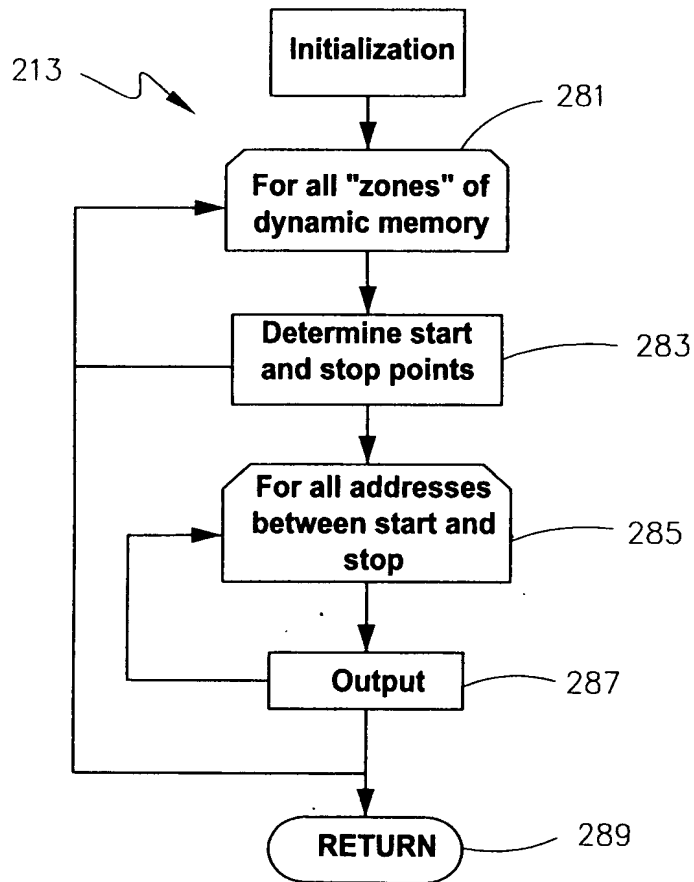


Fig.28a

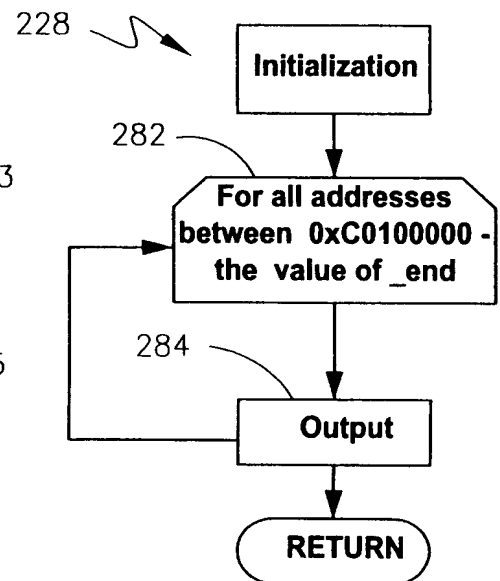


Fig.28c

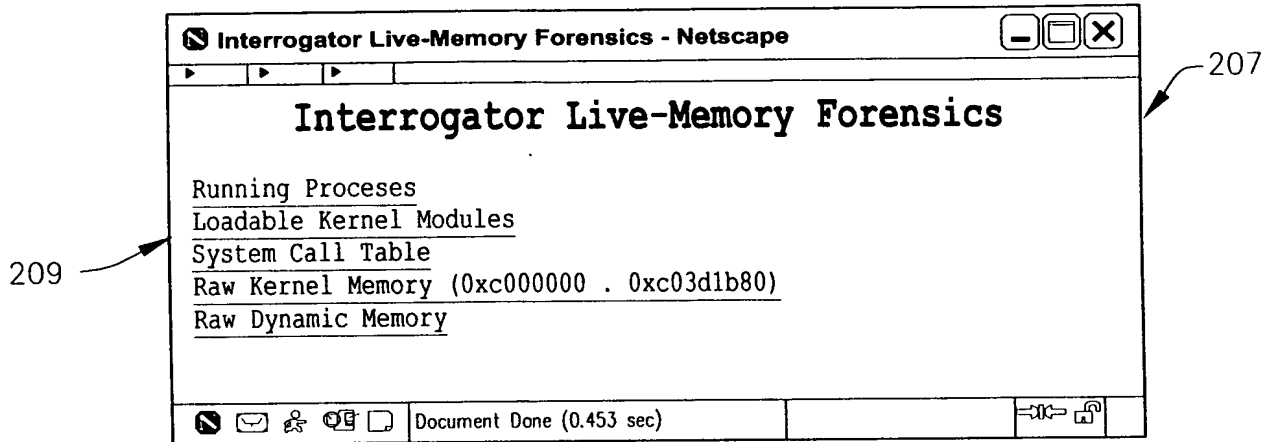


Fig.22b

The screenshot shows a Netscape browser window titled "Loadable Kernel Modules - Netscape". It displays a table of loaded kernel modules. The table has four columns: module name, size, flags, and memory address range. A status bar at the bottom indicates "Document Done (0.25 sec)".

213

215

217

219

211

241

| | | | |
|-----------------|-------|---|-------------------------|
| ide ed | 33608 | 0 | 0xd08e6000 - 0xd08ee348 |
| vmhgfs | 37228 | 4 | 0xd08e0000 - 0xd08f916c |
| ip tables | 14936 | 2 | 0xd08e0000 - 0xd08fea58 |
| iptables filter | 2412 | 1 | 0xd0900000 - 0xd090096c |
| nls iso8859-1 | 3516 | 1 | 0xd0902000 - 0xd0902dbc |
| pcnet32 | 17856 | 1 | 0xd0906000 - 0xd090a5c0 |
| ipt REJECT | 3736 | 6 | 0xd090e000 - 0xd090ee98 |
| autofs | 13348 | 0 | 0xd0910000 - 0xd0913424 |
| soundcore | 6532 | 0 | 0xd0970000 - 0xd0971984 |
| sr mod | 18136 | 0 | 0xd0995000 - 0xd09996d8 |
| usb storage | 62000 | 1 | 0xd09ee000 - 0xd09dd230 |
| fat | 38712 | 0 | 0xd09df000 - 0xd09e8738 |
| vfat | 13084 | 1 | 0xd09ea000 - 0xd09ed31c |
| nls cp437 | 5116 | 1 | 0xd09ef000 - 0xd09f03fc |
| adore | 7968 | 0 | 0xd09f2000 - 0xd09f3f20 |

Fig.25b

261

263

| System Call | Address | NAME |
|-------------|------------|---------|
| Syscall[1] | 0xc011e1d0 | exit |
| Syscall[2] | 0xd09f2650 | fork |
| Syscall[3] | 0xc013fb70 | read |
| Syscall[4] | 0xd09f27e0 | write |
| Syscall[5] | 0xd09f3184 | open |
| Syscall[6] | 0xd09f2898 | close |
| Syscall[7] | 0xc011e560 | waitpad |
| Syscall[8] | 0xc013f180 | creat |
| Syscall[9] | 0xc014cb10 | link |
| Syscall[10] | 0xc015a011 | wait |

Fig.27b

265

265

| Zone | Begin | End |
|---------|------------|------------|
| DMA | 0xc1000030 | 0xc1038030 |
| Normal | 0xc1070030 | 0xc13b8030 |
| Highmem | 0x0 | 0x0 |
| Dynamic | 0xd0800000 | 0xd0900000 |

Fig.28b

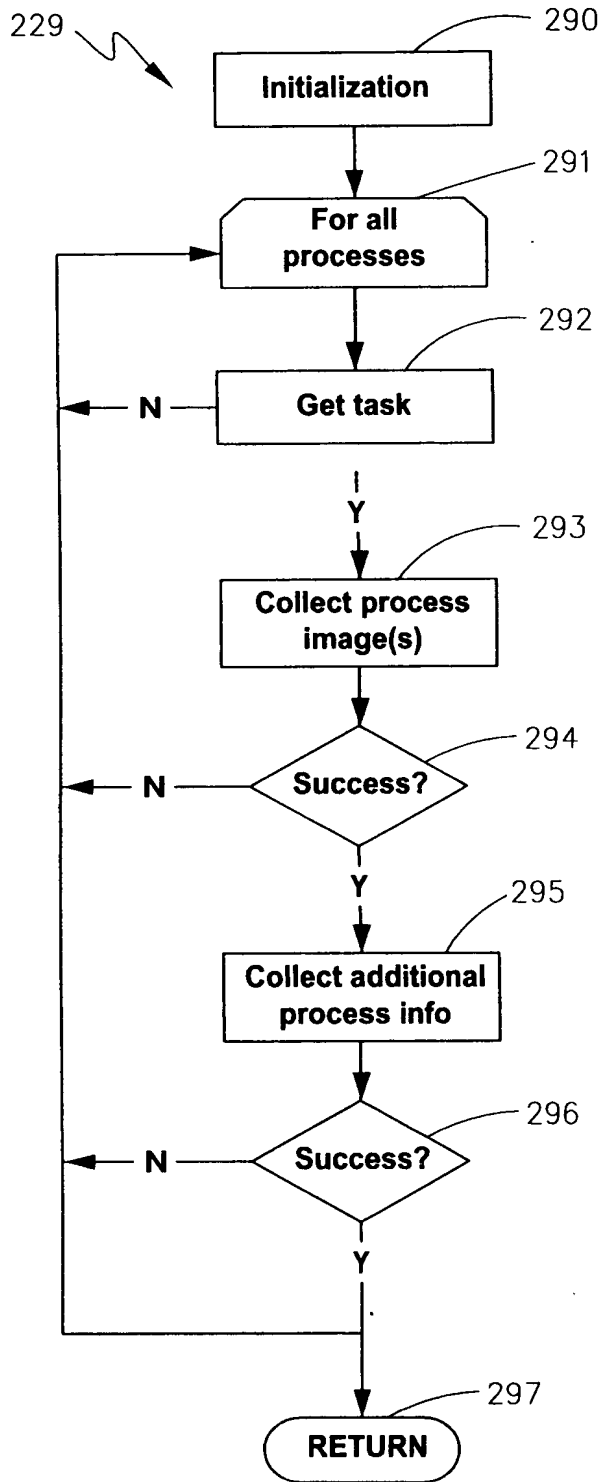


Fig.29a

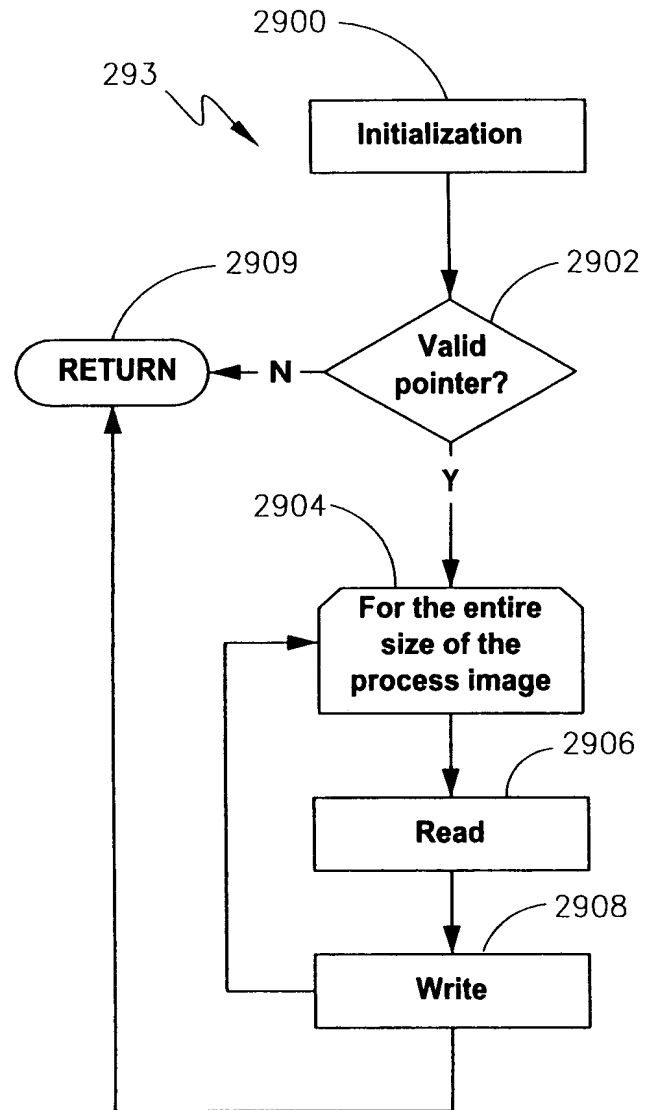


Fig.29b

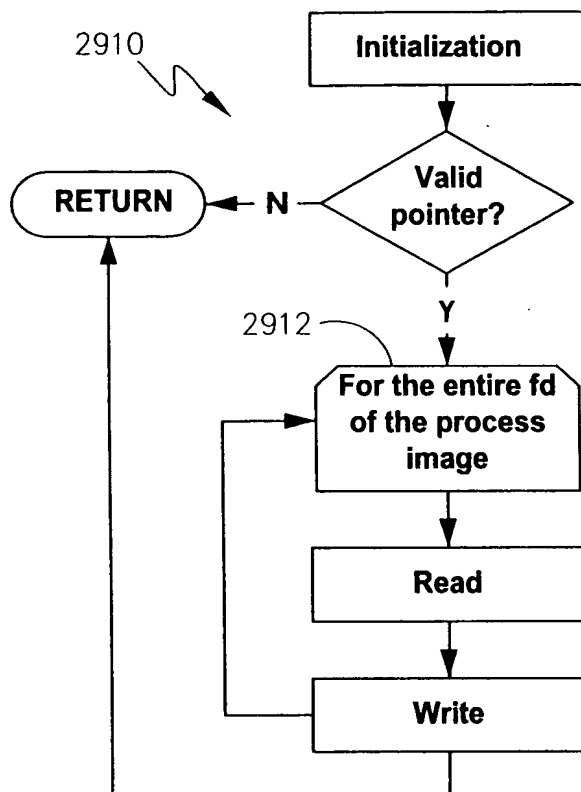


Fig.29c

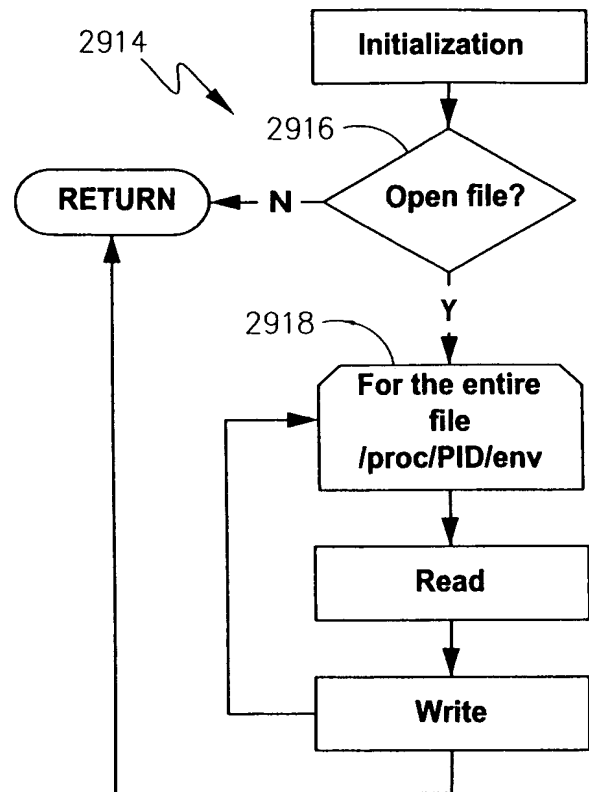


Fig.29d

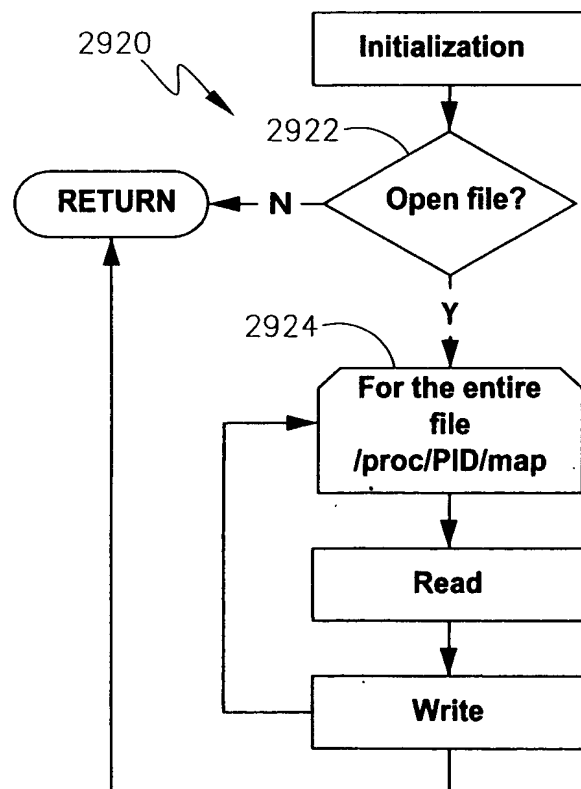


Fig.29e

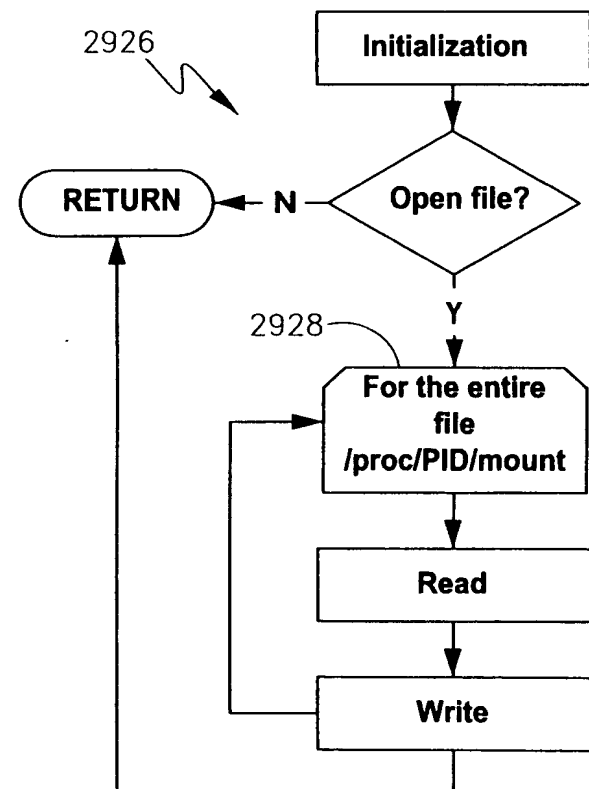


Fig.29f

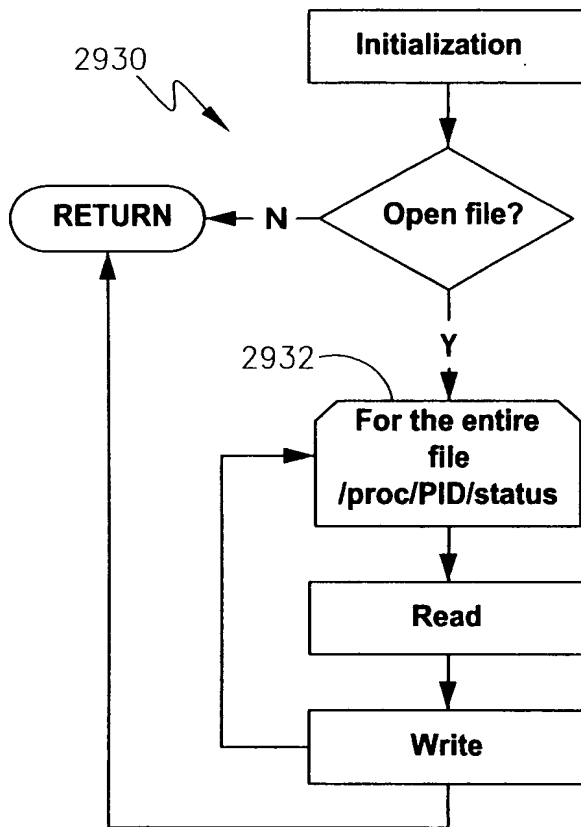


Fig.29g

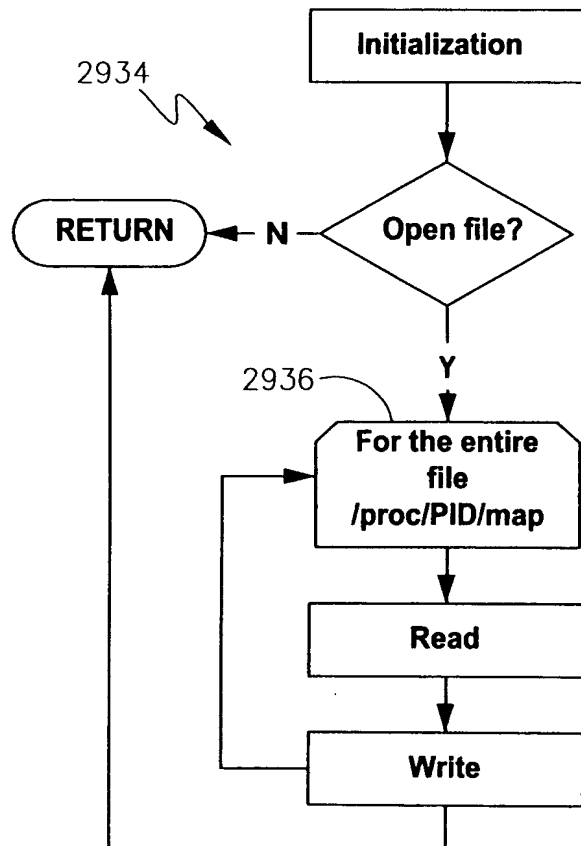


Fig.29h

Loadable Kernel Modules - Netscape

Running Process Listing

| Process | Proc Image | Main Image | File Descriptors | Environment | Mapping | Command | Mounts | Status |
|----------------|------------|------------|------------------|-------------|---------|---------|--------|--------|
| init | 1 | 1 | 0 | env | map | command | mount | status |
| vinware-guestd | 327 | 327 | 4 | env | map | command | mount | status |
| dhcibent | 529 | 529 | 3 | env | map | command | mount | status |
| syslogd | 582 | 582 | 7 | env | map | command | mount | status |
| klogd | 586 | 586 | 2 | env | map | command | mount | status |
| postmap | 603 | 603 | 5 | env | map | command | mount | status |
| rpc.statd | 622 | 622 | 7 | env | map | command | mount | status |
| apend | 703 | 703 | 2 | env | map | command | mount | status |
| sshd | 741 | 741 | 4 | env | map | command | mount | status |
| xinetd | 755 | 755 | 6 | env | map | command | mount | status |
| sendmail | 778 | 778 | 5 | env | map | command | mount | status |
| sendmail | 788 | 788 | 4 | env | map | command | mount | status |
| gpm | 798 | 798 | 2 | env | map | command | mount | status |
| cron | 807 | 807 | 5 | env | map | command | mount | status |
| xfs | 841 | 841 | 6 | env | map | command | mount | status |
| atd | 859 | 859 | 4 | env | map | command | mount | status |
| login | 868 | 868 | 0 | env | map | command | mount | status |

Document Done (0.25 sec)

Fig.29i

total 13696

| | | | | | | |
|------------|----|------|--------|-----|---|-------------------|
| drwxr-xr-x | 2 | root | 4096 | Jan | 5 | 19:41 . |
| drwxr-xr-x | 11 | root | 4096 | Jan | 5 | 22:26 .. |
| -rwxr-xr-x | 1 | root | 33960 | Jan | 5 | 19:40 1.exe |
| -rwxr-xr-x | 1 | root | 33960 | Jan | 5 | 19:40 1.mem_exe |
| -rwxr-xr-x | 1 | root | 103165 | Jan | 5 | 19:40 327.exe |
| -rwxr-xr-x | 1 | root | 103165 | Jan | 5 | 19:40 327.mem_exe |
| -rwxr-xr-x | 1 | root | 390950 | Jan | 5 | 19:40 529.exe |
| -rwxr-xr-x | 1 | root | 390950 | Jan | 5 | 19:40 529.mem_exe |
| -rwxr-xr-x | 1 | root | 33635 | Jan | 5 | 19:40 582.exe |
| -rwxr-xr-x | 1 | root | 33635 | Jan | 5 | 19:40 582.mem_exe |
| -rwxr-xr-x | 1 | root | 28571 | Jan | 5 | 19:40 586.exe |
| -rwxr-xr-x | 1 | root | 28571 | Jan | 5 | 19:40 586.mem_exe |
| -rwxr-xr-x | 1 | root | 40144 | Jan | 5 | 19:40 603.exe |
| -rwxr-xr-x | 1 | root | 38147 | Jan | 5 | 19:40 603.mem_exe |

Fig.30a

| | | | |
|-----|---|------------|-------------------|
| fd: | 0 | READ-WRITE | /socket:/ (1103) |
| fd: | 1 | WRITE-ONLY | /var/log/messages |
| fd: | 2 | WRITE-ONLY | /var/log/secure |
| fd: | 3 | WRITE-ONLY | /var/log/maillog |
| fd: | 4 | WRITE-ONLY | /var/log/cron |
| fd: | 5 | WRITE-ONLY | /var/log/spooler |
| fd: | 6 | WRITE-ONLY | /var/log/boot.log |

Fig.30b

```
SSH_AGENT_PID=4606
HOSTNAME=string-1.internal.vlan.iwc.sytexinc.com
PVM_RSH=/usr/bin/rsh
SHELL=/bin/bash
TERM=xterm
HISTSIZE=1000
GTK_RC_FILES=/etc/gtk/gtkrc:/root//gtkrc-1.2-gnome2
WINDOWID=27270368QTDIR=/usr/lib/qt-3.1
USER=root
LS_COLORS=
PVM_ROOT=/usr/share/pvm3
SSH_AUTH_SOCK=/tmp/sh=XX3Bs0yB/agent.4542
SESSION_MANAGER=local/sring-1.internal.vlan.iwc.sytexinc.com:/tmp/.ICE-
unix/4542
USERNAME=root
MAIL=/var/spool/mail/root
PATH=/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin
:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin:/root/bin:usr/local/netscape
INPUTRC=/etc/inputrc
PWD=/root
XMODIFIERS=@im-none
LANG=en_US.UTF-8
LAMHELPFILE=/etc/lam/lam-helpfile
GDMSESSION=Default
SH_ASKPASS=/usr/libexec/openssh/gnome-ssh-askpass
HOME=/root
SHLVL=2X
PVM_ROOT=/usr/share/pvm3/xpvm
GNOME_DESKTOP_SESSION_ID=Default
BASH_ENV=/root/.bashrc
LOGNAME=root
LESSOPEN=|/usr/bin/lesspipe.sh %s
DISPLAY=:0.0G
BROKEN_FILENAMES=1
COLORTERM=gnome-terminal
XAUTHORITY=/root/.Xauthority=/usr/bin/ssh
```

Fig.30c

```
rootfs / rootfs rw 0 0
/dev/root / ext3 ro 0 0
/proc /proc proc rw 0 0
usbdevfs /proc/bus/usb usbdevfs rw 0 0
/dev/sdal /boot ext3 rw 0 0
none /dev/pts devpts rw 0 0
none /dev/shm tmpfs rw 0 0
none /mnt/hgfs vmware-hgfs rw,nosuid,nodev 0 0
/dev/sdbl /mnt vfat rw 0 0
```

Fig.30d

```
Name: vmware-guestd
State: R (running)
Tgid: 327
Pid: 327
PPid: 1
TracePid: 0
Uid: 0 0 0 0
Gid: 0 0 0 0
FDSize: 32
Groups:
VmSize: 1424 kb
VmLck: 0kb
VmRSS: 444 kb
VmData: 48 kb
VmStk: 8 kb
VmExe: 84 kb
VmLib: 1252 kb
SigPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 8000000000000000
SigCgt: 0000000000004a07
CapIng: 0000000000000000
CapPrm: 00000000fffffffeff
CapEff: 00000000fffffffeff
```

Fig.30e

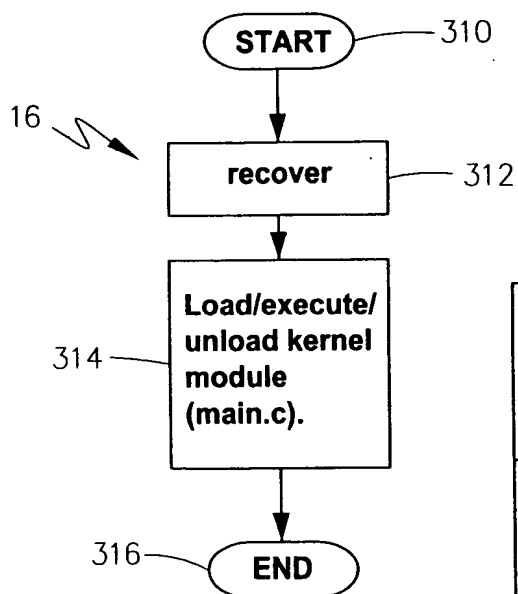


Fig.31

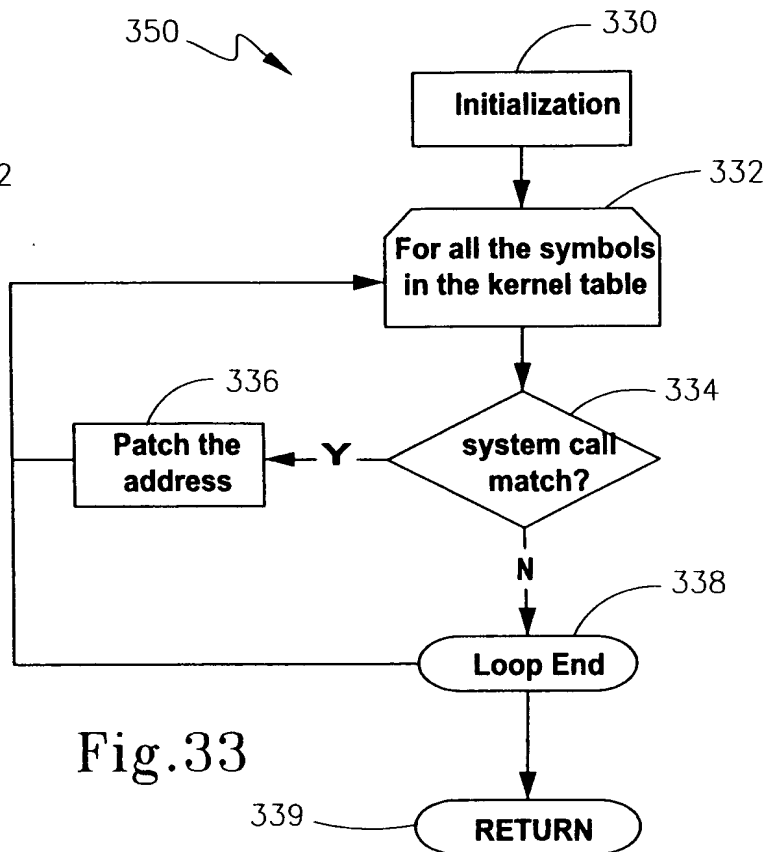


Fig.33

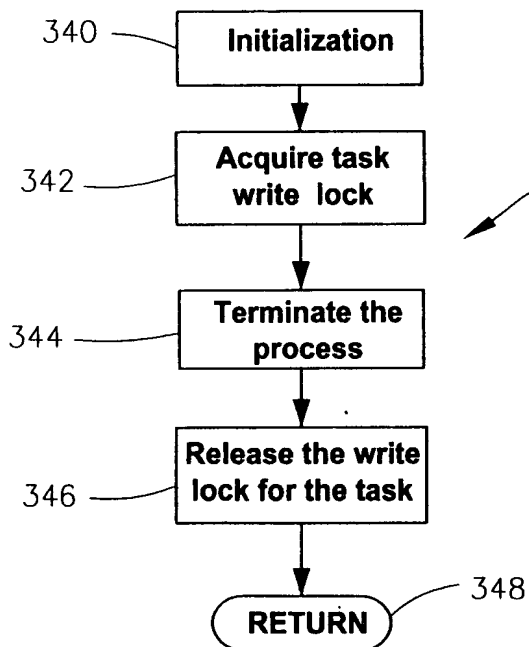


Fig.34

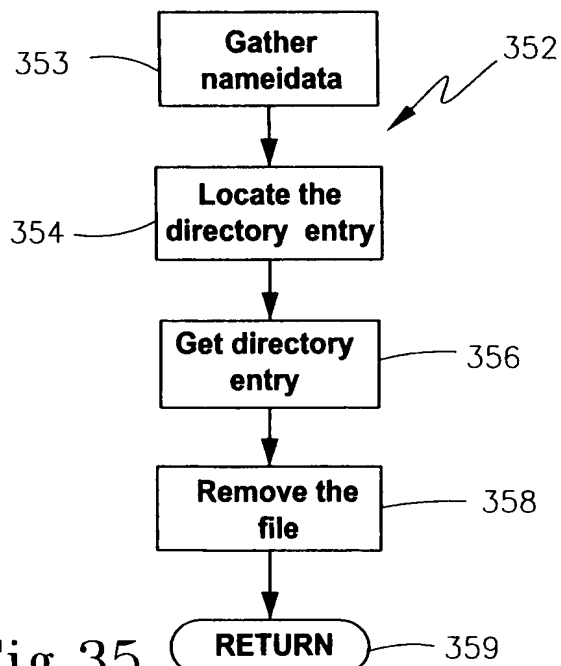


Fig.35

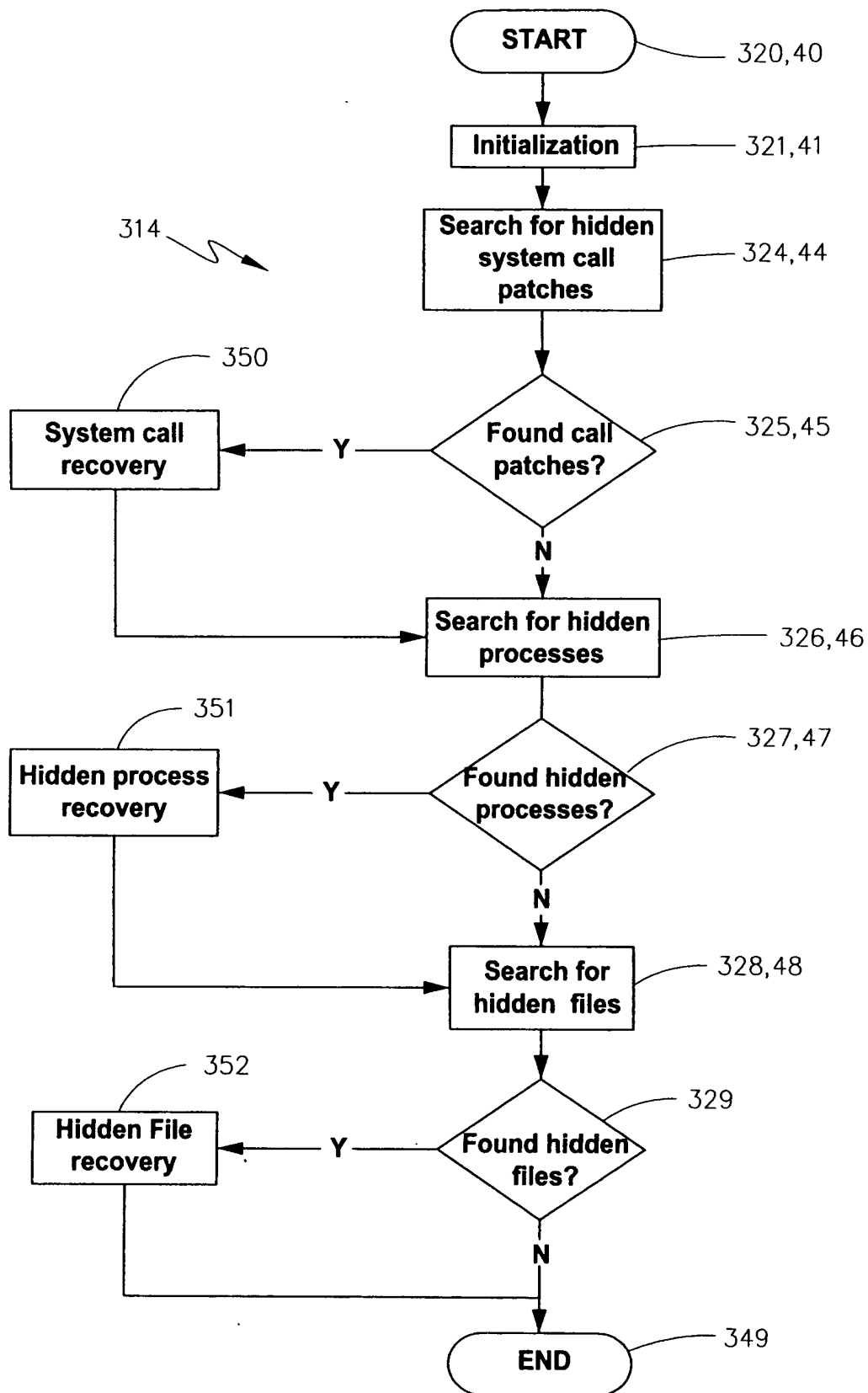


Fig. 32



```
Script started on Sun Jan 11 10:18:52 2004
(root@local.host recovery)# ./recovery
Terminate hidden processes? [Y]
Recover system call table? [Y]
Remove hidden files [N] Y
Results are located at /tmp/interrogator/summary
View results now? [Y]
```

```
-----[ SUMMARY ]-----
NO system call table modifications were found
NO hidden processes were found
(root@local.host recovery)# exit
Script done on Sun Jan 11 10:19:03 2004
```

Fig.36a

```
Script started on Sun Jan 11 10:31:02 2004
(root@local.host adore)# ./startadore
Warning: loading cleaner.o will taint the kernel: no license
See http://www.tux.org/lkml/#export-tainted for information about tainted
modules
Module cleaner loaded, with warnings

(root@localhost adore)# /tmp/test
(root@localhost adore)# ps -ef |grep test
root      1302 1276 0 10:35 pts/3      00:00:00 /tmp/test
root      1304 1043 0 10:35 pts/1      00:00:00 grep test

(root@localhost adore)# ./ava i 1302
Checking for adore 0.12 or higher ...
Adore 0.42 installed. Good luck.
Made PID 1302 invisible.

(root@localhost adore)# ./ava h /tmp/test
Checking for adore 0.12 or higher ...
Adore 0.42 installed. Good luck.
File '/tmp/test' hided.

(root@localhost adore)# ls /tmp
ssh-XXAbSIW
ssh-XXEZXD3

(root@localhost adore)# ps -ef |grep test
(root@localhost adore)# exit
Script done on Sun Jan 11 10:35:40 2004
```

Fig.36b

```
Script started on Sun Jan 11 10:52:37 2004
(root@local.host recovery)# ./recovery
Terminate hidden processes? [Y]
Recover system call table? [Y]
Remove hidden files [N]. Y
Results are located at /tmp/interrogator/summary
View results now? [Y]

-----[ SUMMARY ]-----
WARNING: process id 1302 hidden or just exited (test)
Launch Path: /tmp/test
TERMINATED 1 Hidden process listing
(root@local.host recovery)# exit
Script done on Sun Jan 11 10:54:26 2004
```




Fig.36c

```
Script started on Sun Jan 11 10:35:21 2004
(root@local.host recovery)# /tmp/test
Running 1
Running 2
Running 3
Running 4
Running 5
Running 6
Running 7
Hangup
Script done on Sun Jan 11 10:55:12 2004
```




Fig.36d

Script started on Sun Jan 11 10:57:09 2004

[root@localhost recovery]# ls /tmp

ssh-XXAbs7W

ssh-XXB2XD3

[root@localhost recovery]# sum /tmp/test

03965 12

[root@localhost recovery]# ./recover

Terminate hidden processes? [Y] N

Recover system call table? [Y] N

Delete hidden files? [N] Y

Results are located at /tmp/interrogator/summary

View results now? [Y]

-----[SUMMARY]-----

REMOVED /tmp/test

(root@localhost recovery]# ls /tmp

ssh-XXAbs7W

ssh-XXEZXD3

{root@localhost recovery]# sum /tmp/test

sum: /tmp/test: No such file or directory

root@localhost recovery]# exit

Script done on Sun Jan 11 10:57:47 2004

364
↙

Fig.36e

```
Script started on Sun Jan 11 10:57:57 2004
[root@localhost recovery] # ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y]
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary

View results now? [Y]
```


```
-----[ SUMMARY ]-----
```

```
WARNING suspect module found: d09cb000 7968 bytes (adore)
FOUND 1 HIDDEN module loaded
```

```
WARNING: Deviations found in the sys_call_table
```

| | | | |
|--------------|--------|------------|------------|
| syscall[2] | FAILED | Oxd09cb650 | fork |
| syscall[4] | FAILED | Oxd09cb7e8 | write |
| syscall[5] | FAILED | Oxd09cc184 | open |
| syscall[6] | FAILED | Oxd09cb898 | close |
| syscall[18] | FAILED | Oxd09cbbe4 | stat |
| syscall[37] | FAILED | Oxd09cb710 | kill |
| syscall[39] | FAILED | Oxd09cb9a0 | mkdir |
| syscall[84] | FAILED | Oxd09cbcd0 | Istat |
| syscall[106] | FAILED | Oxd09cbdbc | stat |
| syscall[107] | FAILED | Oxd09cbe94 | Istat |
| syscall[120] | FAILED | Oxd09cb6b0 | clone |
| syscall[141] | FAILED | Oxd09cb368 | getdents |
| syscall[195] | FAILED | Oxd09cbf80 | stat64 |
| syscall[196] | FAILED | Oxd09cc080 | lstat64 |
| syscall[220] | FAILED | Oxd09cb4dc | getdents64 |

RECOVERED 15 Modified syscall table functions



```
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y]
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary
View results now? [Y]
```

```
-----[ SUMMARY ]-----
```

```
NO system call table modifications were found.
```

Fig.36f

```
Script started on Sun Jan 11 11:31:47 2004
[root@localhost adore]# ps -ef |grep test
root    1284 1258 0 11:31 pts/1    00:00:00 /tmp/test

[root@localhost adore]# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3
test

[root@localhost adore]# ./startadore
Warning: loading cleaner.o will taint the kernel: no license
See http://www.tux.org/lkml/#export-tainted for information about tainted
modules
Module cleaner loaded, with warnings

[root@localhost adore]# ./ava i 1284
Checking for adore 0.12 or higher ...
Adore 0.42 installed. Good luck.
Made PID 1284 invisible.

[root@localhost adore]# ./ava h /tmp/test
Checking for adore 0.12 or higher ...
Adore 0.42 installed. Good luck.
File '/tmp/test' hided.

(root@localhost adore)# ps -ef |grep test
(root@localhost adore)# ls /tmp
ssh-XXAbS7W
ssh-XXEZXD3

[root@localhost adore]# cd ../interrogator/recovery
[root@localhost recovery]# ./recover
Terminate hidden processes? [Y] N
Recover system call table? [Y] Y
Delete hidden files? [N] N
Results are located at /tmp/interrogator/summary
View results now? [Y]
-----[ SUMMARY ]-----
WARNING suspect module found: d09cb000 7968 bytes (adore)
FOUND 1 HIDDEN module loaded

WARNING: Deviations found in the sys_call_table
syscall[2]      FAILED 0xd09cb650    fork
syscall[4]      FAILED 0xd09cb7e8    write
syscall[5]      FAILED 0xd09cc184    open
syscall[6]      FAILED 0xd09cb898    close
syscall[18]     FAILED 0xd09cbbe4    stat
syscall[37]     FAILED 0xd09cb710    kill
syscall[39]     FAILED 0xd09cb9a0    mkdir
syscall[84]     FAILED 0xd09cbcd0    lstat
syscall[106]    FAILED 0xd09cbdbc    stat
syscall[107]    FAILED 0xd09cbe94    lstat
syscall[120]    FAILED 0xd09cb6b0    clone
syscall[141]    FAILED 0xd09cb368    getdents
syscall[195]    FAILED 0xd09cbf80    stat64
syscall[196]    FAILED 0xd09cc080    lstat64
syscall[220]    FAILED 0xd09cb4dc    getdents64
RECOVERED 15 Modified syscall table functions

[root@localhost recovery]# ps -ef |grep test
root      1284 1258 0 11:31 pts/1    00:00:00 /tmp/test
root      1345 1288 0 11:33 pts/2    00:00:00 grep test

[root@localhost recovery]# ls /tmp
ssh-XXAbS7W
ssh-XXS2XD3
test

[root@localhost recovery]# exit

Script done on Sun Jan 11 11:33:21 2004
```

366



Fig.36g